BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC HOA SEN
KHOA KHOA HỌC VÀ CÔNG NGHỆ

KHÓA LUẬN TỐT NGHIỆP

Tên đề tài: FIREWALL CHECKPOINT

Giảng viên hướng dẫn : Thầy Đinh Ngọc Luyện
Nhóm sinh viên thực hiện : Cao Hiệp Hưng MSSV : 070112
Lương Hữu Tân MSSV : 070057
Lớp : VT071

Tháng 12 /năm 2010

TRÍCH YẾU

Thông qua Khóa Luận Tốt Nghiệp, về cơ bản chúng tôi đã nghiên cứu về những vấn đề sau

- Xây dựng hệ thống Firewall cùng chính sách bảo mật cho mạng.
- Thiết lập các phương thức kết nối an toàn trong mạng Internet (IPsec VPN).
- Xây dựng hệ thống quản lý sự truy xuất mạng và đảm bảo người dùng có thể truy xuất chính xác dữ liệu theo đúng quyền hạn và vị trí của họ. Đồng thời tối ưu hóa tối độ truy cập và tránh rủi ro mất mát dữ liệu.

Và kết quả đạt được là có được kiến thức về các thiết bị Checkpoint, hiểu được quy tắc hoạt động, truyền thông của các thiết bị Checkpoint cùng những giao thức chạy trên chính các thiết bị đó.

Nắm được quy tắc cấu hình, quản lý và bảo trì thiết bị Checkpoint.

Có được kiến thức về khả năng tương tác giữa thiết bị của Chekpoint với thiết bị, phần mềm của những hãng khác (Cisco, Microsoft, Juniper Network…).

Tận dụng được các chức năng tương tác giữa các thiết bị đảm nhận vai trò khác nhau (IPS cùng Firewall, Switch cùng Security Gateway…).

Có được kiến thức về các loại tấn công đối với hệ thống mạng và hệ thống máy local (Worm, Trojan, Virus…).

Hiểu và ứng dụng những công nghệ bảo mật tiên tiến của Checkpoint vào quá trình xây dựng và quản lý hệ thống.
Ngoài ra chúng tôi còn có thêm được kỹ năng về làm việc nhóm, kỹ năng phân chia công việc, nhiệm vụ, thời gian hợp lý.

MỤC LỤC

LỜI CÁM ƠN

Đầu tiên, chúng tôi xin cám ơn trường Đại học Hoa Sen đã tạo cơ hội cho chúng tôi thực hiện Khóa Luận Tốt Nghiệp này để chúng tôi có cơ hội tìm hiểu thêm nhiều kiến thức mới, có ích cho công việc chúng tôi sau khi tốt nghiệp.

Và chúng tôi cũng xin cám ơn thầy Đinh Ngọc Luyện đã tạo cơ hội cho chúng tôi thực hiện Khóa Luận Tốt Nghiệp này, thầy đã hướng dẫn, cung cấp tài liệu, hỗ trợ về mặt tinh thần để chúng tôi có thể hoàn thành tốt Khóa Luận Tốt Nghiệp, giúp chúng tôi có nhiều kinh nghiệm thực tế hơn về phương diện làm việc nhóm và những kiến thức cấu hình thiết bị trong thực tiễn.
Xin cám ơn các thầy cô ở phòng Đào tạo đã hỗ trợ chúng tôi về những thông tin cần thiết về Khóa Luận Tốt Nghiệp.

NHẬN XÉT CỦA GIẢNG VIÊN

CHAPTER 01 – VPN
VIRTUAL PRIVATE NETWORK

Trong chapter này ta sẽ nói về Virtual Private Network và những vấn đề liên quan.

Chapter 01 – Virtual Private Network bao gồm ba phần

- *Cryptography*
- *IPsec VPN and IPsec Site-to-Site VPN*
- *IPsec Remote Access VPN*

❖ Cryptography

Phần Cryptography sẽ những thuật toán mã hóa cổ điển, những thuật toán mã hóa hiện đại và các phương pháp bẻ gãy mã.

Đặc điểm và mục đích sử dụng của các thuật toán HASH.

Đặc điểm và mục đích sử dụng của các thuật toán mã hóa.

Cuối cùng là chữ ký số và kiến trúc PKI.

- Classic Cryptography
- Modern Cryptography
- Cryptanalysis
- PKI – Public Key Infrastructure

❖ IPsec VPN

Trong phần này ta sẽ nói về VPN và những lợi ích của VPN so với các kiểu kết nối cũ.

Giới thiệu về IPsec VPN và các chức năng của IPsec VPN. Bên cạnh đó là giới thiệu các giao thức bảo mật của IPsec.

Đi sâu vào phân tích quá trình đàm phán ở IKE Phase I và IKE Phase II.

Cuối cùng là các vấn đề khác khi thiết lập đường IPsec Site-to-Site VPN.

- VPN Overview
- IPsec VPN
- VPN Communities and Terminology

- IKE DoS Attack and Checkpoint Solution
- VPN Topologies
- Access Control Policy and VPN Communities

❖ IPsec Remote Access VPN

Trong phần này ta sẽ nói về IPsec Remote Access VPN cùng các chức năng của IPsec Remote Acces VPN.

Bên cạnh đó là những vấn đề có thể phát sinh của Remote User khi dùng IPsec Remote Access.

Cuối cùng các các chế độ làm việc của Remote Access VPN.

- Overview
- Resolving Connectivity Issues
- Office Mode
- Remote Access Routing

A . Cryptography

Cách đây hơn 5000 năm, ngành mật mã học đã ra đời. Đây là ngành liên quan tới việc sử dụng các ngôn ngữ và các thuật toán để đảm bảo an toàn cho thông tin. Thông tin ban đầu được gọi là cleartext hay plaintext, sau khi được mã hóa sẽ trở thành ciphertext - là dạng thông tin không thể hiểu được.

Ngành mật mã học chú trọng tới hai vấn đề chính

- Mã hóa – Cryptography.
- Giải mã hay bẻ khóa mã – Cryptanalysis.

1 Classic Cryptography

Trong lịch sử, mật mã dùng để bảo vệ các thông tin về quân sự, tình báo, ngoại giao…

1.1 Substitution Cipher

Substitution Cipher - thay thế ký tự, đây là phương pháp được dùng bởi Julius Caesar nên còn được gọi là Caesar Cipher.

Ở phương pháp này, ta sẽ thay thế ký tự này bởi ký tự khác theo một quy tắc nhất định. Và người gửi sẽ quy định một key với người nhận để người nhận có thể giải mã đúng ra thông tin plaintext ban đầu.

Điểm yếu của phương pháp này là có thể dễ dàng bị giải mã bằng phương pháp thử liên tục, cho đến khi tìm được key cần thiết.

1.2 Vigenère Cipher

Vigenère Cipher – Polyalphabetic Cipher là phương pháp có cùng ý tưởng thay thế ký tự như ở Caesar Cipher, nhưng phương pháp này phức tạp hơn và cần nhiều thời gian để giải mã hơn.

1.3 Transposition

Transposition – Hoán vị, đây là phương pháp này thì các ký tự trong chuỗi plaintext ban đầu sẽ được hoán vị để tạo ra chuỗi ciphertext.

2 Modern Cryptography

Các phương pháp mã hóa hiện tại sẽ được phân chia thành hai mảng lớn

- *Encryption – Mã hóa : Đảm bảo tính bí mật (Confidentiality).*
- *Hash – Băm : Đảm bảo tính toàn vẹn dữ liệu (Data Integity).*

2.1 Hash

2.1.1 Hash Overview

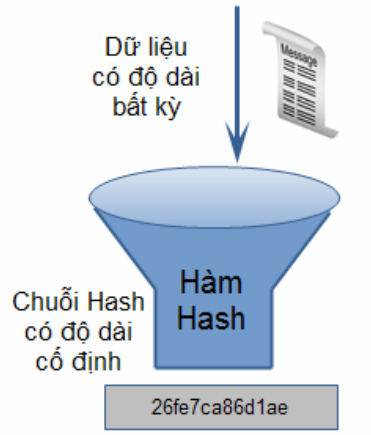
Hash thường được sử dụng để đảm bảo tính toàn vẹn dữ liệu (Data Integity).

Hash là One-way Function (Hàm một chiều) : Đảm bảo dữ liệu sau khi được hash sẽ không thể truy ngược ra lại thành dữ liệu như ban đầu.

Dữ liệu bất kỳ sau khi được hash sẽ trở thành một chuỗi ký tự có độ dài không đổi tùy thuộc vào thuật toán và được gọi là Fingerprint.

Avalanche Effect : Khi có bất kỳ sự thay đổi nhỏ nào ở dữ liệu, thì Fingerprint sẽ thay đổi rất nhiều.

Các yếu tố của hàm Hash



- Input là dữ liệu có độ dài bất kỳ.
- Output là chuỗi đã được Hash(Fingerprint) có độ dài xác định.
- Hàm Hash có thể làm việc với bất kỳ Input nào.
- Hàm Hash sẽ cho ra kết quả một chiều – Oneway và không thể truy ngược lại.
- Hàm Hash là collision-free (Không thể tìm ra 2 input để cho ra 1 output giống nhau).

Hình A1 – 1 : Hash Function

Hacker hoàn toàn có thể thấy được nội dung của dữ liệu khi nó được truyền. Hay nói cách khác Hash không cung cấp tính bí mật cho dữ liệu được truyền (Confidentiality).

Hash có thể bị tấn công bằng Man-in-the-middle (Bằng cách thay đổi thông tin dữ liệu và chèn 1 chuỗi hash giả dựa trên dữ liệu đã được thay đổi).

Hai hàm hash được sử dụng nhiều là MD5 và SHA-1.

- MD5 có 128bits khi hash.
- SHA-1 có 160bits khi hash.

2.1.1.1 MD5 – Message Digest 5

Đây là thuật toán Hash thường được sử dụng với ưu điểm là tốc độ tính toán nhanh và không thể truy ngược lại data trước khi Hash (One-way function).

Collision resistant –Hai dữ liệu khác nhau sẽ cho ra cùng một chuỗi Hash là điều không thể xảy ra.

Sử dụng 128bits Hash.

Tuy nhiên với độ dài của chuỗi Hash thì MD5 đã không còn thích hợp cho các ứng dụng bảo mật mới.

2.1.1.2 SHA – Secure Hash Algorithm

Có chức năng gần giống MD4 hay MD5 với dữ liệu Input không quá 2^{64} bits.

Sử dụng 160bits Hash.

Tốc độ tính toán chậm hơn MD5.

2.1.2 HMAC – Hashed Message Authentication Code

Với HMAC thì dữ liệu sẽ đi vào hàm Hash cùng với một secret key để tăng độ bảo mật của hàm Hash.

Secret key này chỉ được chia sẻ giữa người nhận và người gửi.

HMAC sẽ loại bỏ hoàn toàn kiểu tấn công Man-in-the-middle.

HMAC hoạt động dựa trên các hàm Hash có sẵn như MD5 hay SHA-1.

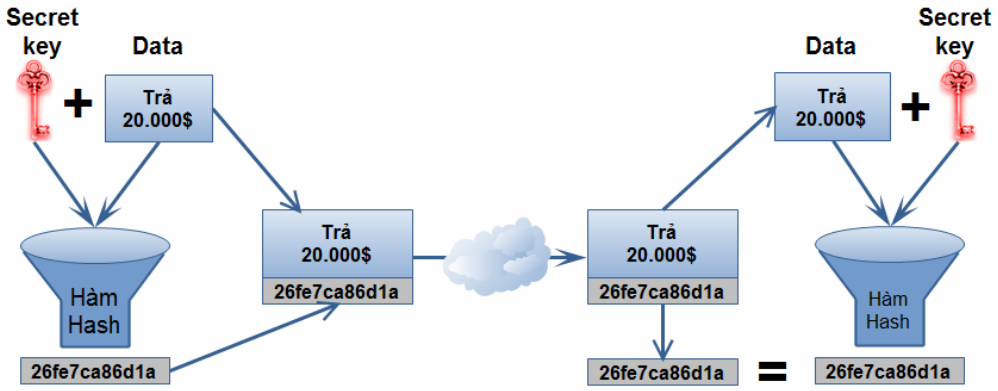
❖ Quy tắc kiểm tra

Bước 1 : Dữ liệu sẽ được đưa vào hàm Hash cùng với *secret key*.

Bước 2 : Dữ liệu khi gửi đi sẽ được dính kèm với chuỗi Hash.

Bước 3 : Bên nhận khi có được dữ liệu sẽ đưa vào hàm Hash cùng với *secret key* tương tự như bên gửi để có chuỗi Hash thứ hai.

Bước 4 : Bên nhận dữ liệu sẽ so sánh chuỗi hash nhận được và chuỗi hash do chính bên nhận tạo ra. Nếu giống nhau thì dữ liệu không bị thay đổi. Ngược lại nếu có sự thay đổi thì hai chuỗi Hash sẽ khác nhau.



Hình A1 – 2 : HMAC Function Example

2.2 Encryption

2.2.1 Encryption overview

Để chống lại rủi ro dữ liệu có thể bị đọc lén trong quá trình truyền trên mạng, ta cần phải có một phương pháp để đảm bảo tính bí mật của dữ liệu. Từ đó ta có mã hóa dữ liệu.

Trong các thuật toán mã hóa hiện tại thì điều mong muốn hàng đầu đó là

- Chống lại các thuật toán phá mã, các dạng tấn công mã.
- Key có độ dài lớn và có khả năng mở rộng key.
- Hiệu ứng thác – Avalanche Effect : Khi có bất kỳ một sự thay đổi nhỏ nào ở plaintext đều dẫn tới sự thay đổi rất lớn ở ciphertext tương ứng.
- Không có sự giới hạn giữa việc nhập và xuất.

Dựa theo cách dữ liệu được mã hóa và sử dụng key, mà ta sẽ có hai cách phân loại.

- Dựa theo cách sử dụng key
  - + Symmetric Encryption Algorithms – Thuật toán mã hóa đồng bộ.
  - + Asymmetric Encryption Algorithms – Thuật toán mã hóa bất đồng bộ.
- Dựa theo cách dữ liệu được mã hóa
  - + Block ciphers.
  - + Stream ciphers.

2.2.2 Block and Stream cipher

2.2.2.1 Block cipher

- Là cách mà plaintext sẽ được encrypted theo từng Block giống nhau về độ dài để tạo ra các Block cipher tương ứng.
- Tùy thuộc vào thuật toán mà Block sẽ có độ lớn khác nhau (DES là 8bytes, AES là 16bytes, RC6 là 16bytes…).
- Padding (dữ liệu đệm) sẽ giữ cho kích thước của dữ liệu luôn là bội số của kích thước block (Bằng cách chèn thêm các dummy bits).
- Ciphertext luôn có kích thước lớn hơn plaintext tương ứng.

2.2.2.2 Stream cipher

- Stream cipher sẽ encrypted plaintext theo từng đơn vị nhỏ như là các bits.
- Kích thước của ciphertext thường không khác gì so với plaintext tương ứng.

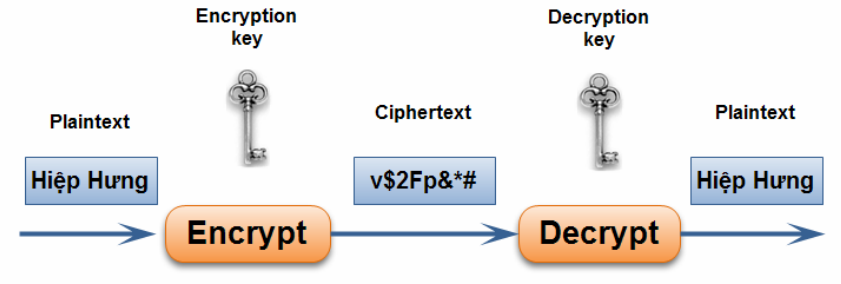
2.2.3 Symmetric Encryption Algorithms

2.2.3.1 Symmetric Encryption Allgorithms Overview

Symmetric Encryption Algorithms là các thuật toán sử dụng cùng một key để encrypted lẫn decrypted dữ liệu. Như vậy thì ta cần phải chia sẻ cùng một secret key cho cả hai phía gửi và nhận.

❖ Quy tắc

- Hai bên gửi/nhận sử dùng cùng một private key và thuật toán giống nhau.
- Người gửi sẻ sử dụng private key để encrypted thông tin plaintext thành ciphertext.
- Người nhận sử dụng private key giống bên phía người gửi để decrypted ciphertext thành plaintext.



Hình A1 – 3 : Symmetric Encryption Algorithm

❖ Ưu điểm

- Tốc độ encrypted/decrypted nhanh hơn các thuật toán mã hóa bất đồng bộ.
- Sử dụng key có chiều dài ngắn hơn các thuật toán mã hóa bất đồng bộ.
- Ít hao tốn tài nguyên hệ thống.
- Các quy tắc tính toán trong thuật toán mã hóa đồng bộ dễ hơn trong các thuận toán mã hóa bất đồng bộ.
- Sử dụng cùng một key để encrypted/decrypted.
- Rất khó và tốn nhiều thời gian để giải mã nếu không có key để decrypted.

❖ Nhược điểm

- Việc bảo mật key là một thử thách lớn, do đó cần phải có phương pháp trao đổi key an toàn hoặc truyền qua Out-of-band.
- Giới hạn số lượng người sử dụng.

Độ dài của key được sử dụng là từ 40-256 bits.

Key được xem là an toàn khi có độ dài hơn 80 bits.

Một số thuật toán mã hóa đồng bộ : DES, 3DES, AES, RC2/4/5/6 và Blowfish.

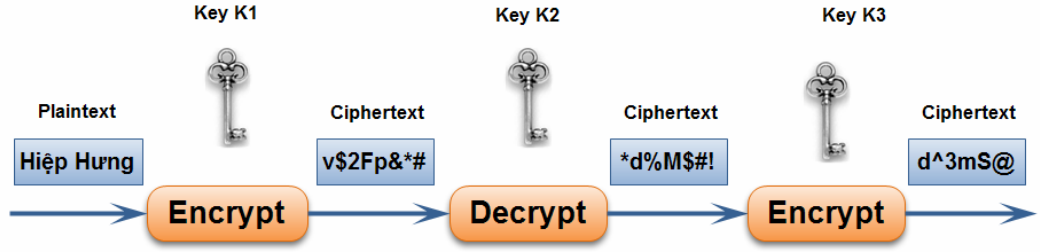
2.2.3.2 DES (Data Encryption Standard)

- Sử dụng key có chiều dài cố định là 64 bits với 56 bits được dùng để encrypted và 8 bits dùng kiểm tra lỗi. Nhưng thật chất chiều dài key của DES chỉ là 40 bits do 56bits được dùng để encrypted thì có 16 bits đã được biết trước – known bits.
- DES là dạng Block cipher 64bits với hai chế độ
  + ECB mode - Electronic Code Book : Mỗi plaintext block khi encrypted sẽ cho ra ciphertext block tương ứng.
  + CBC mode - Cipher Block Chaining: Mỗi plaintext block sẽ được XOR với ciphertext liền trước nó rồi mới được encrypted.
- DES còn là dạng Stream cipher với hai chế độ
  + CFB mode - Cipher Feedback.
  + OFB mode - Output Feedback.

- Nên thay đổi key thường xuyên khi dùng thuật toán này để tránh bị tấn công Bruteforce.
- Private key cần được gửi trên một kênh bảo mật.
- Nên sử dụng CBC mode thay vì ECB mode.
- Do sử dụng các giải thuật đơn giản nên DES dễ triển khai trên hardware.

2.2.3.3 Tri-DES

- Thuật toán 3DES dựa trên nền tảng của thuật toán DES. Sự khác biệt chính đó là 3DES sử dụng bộ gồm ba key để đạt được độ dài key là 168 bits.
- Bộ key gồm ba key K1 – K2 – K3 với
  + Key K1 để encrypted plaintext ban đầu.
  + Key K2 để decrypted phần ciphertext có được khi encrypted bằng Key K1.
  + Key K3 để encrypted phần ciphertext có được khi decrypted bằng Key K2.



Hình A1 – 4 : Tri-DES Algorithm

- Do độ dài của key là rất lớn nên việc bẻ khóa lẫn thời gian bẻ khóa là điều không tưởng đối với việc thay đổi key thường xuyên, nên thuật toán này được xem là một trong những thuật toán mã hóa đồng bộ đáng tin tưởng nhất.

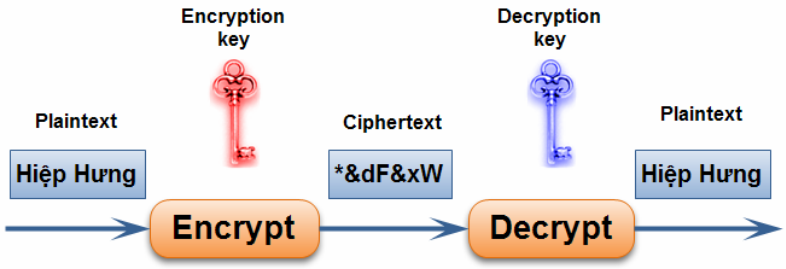
2.2.3.4 AES (Advanced Encryption Standard)

- AES là dự án ra đời vào năm 1998 với mục đích tìm thuật toán thay thế cho DES. Và cuối cùng thì thuật toán Rijndael (của Vincent Rijmen và Joan Daemen) là ứng cử viên tốt nhất.
- Rijndael có tốc độ nhanh hơn 3DES khi chạy trên nền software.
- AES sử dụng key và data block có độ dài khác nhau với số bit là bội của 32.
- Độ dài của key thường là 128/192/256 bits để encrypted các data block có độ dài 128/192/256 bits.
- Sau 10 năm ra đời thì AES chưa hề có một lỗ hổng nào.

2.2.4 Asymmetric Encryption Algorithms

2.2.4.1 Asymmetric Encryption Algorithms Overview

Asymmetric Encryption Algorithms là các thuật toán sử dụng một key để encrypted và một key khác để decrypted. Như vậy cả hai phía gửi/nhận sẽ phải tạo ra bộ key gồm Public key/Private key để dùng cho việc encrypted/decrypted.



Hình A1 – 5 : Asymmetric Encryption Algorithm

Độ dài của key được sử dụng là từ 512 – 4096 bits.

Key được xem là an toàn khi có độ dài hơn 1024 bits.

❖ Ưu điểm

- Do việc key được sử dụng để encrypted khác với key sử dụng cho decrypted, nên việc truyền một trong hai key trên môi trường untrust được xem như là an toàn để trao đổi dữ liệu.
- Các thuật toán mã hóa bất đồng bộ được dùng như là môi trường an toàn để vận chuyển key của thuật toán mã hóa đồng bộ.

❖ Nhược điểm

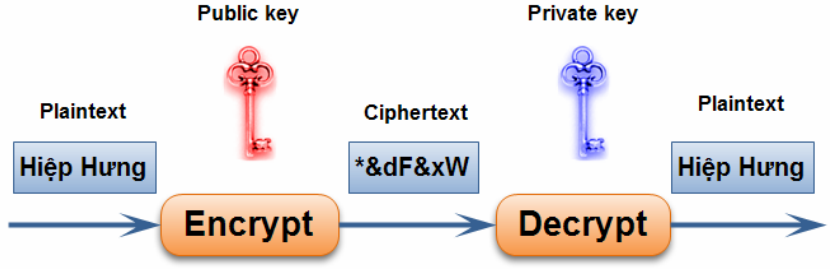
- Do sử dụng các giải thuật phức tạp nên việc tạo key, quá trình encrypted/decrypted sẽ chậm và tốn nhiều thời gian.
- Do Public key và Private key được cùng tạo ra và có mối quan hệ với nhau, nên việc giải mã bộ key này là điều hoàn toàn có thể dù key rất dài.

Tùy vào một đích sử dụng mà quá trình encrypted sẽ dùng Private key hay Public key, tương tự với quá trình decrypted.

Một số thuật toán mã hóa đồng bộ RSA, DSA, DH, ElGamal, Elliptic Curve…

2.2.4.2 Public Key Confidentiality – Bảo mật bằng Public key

Ở cơ chế này thì Public key sẽ được dùng để encrypted thông tin thành ciphertext và Private key tương ứng được dùng để decrypted ciphertext thành thông tin ban đầu.



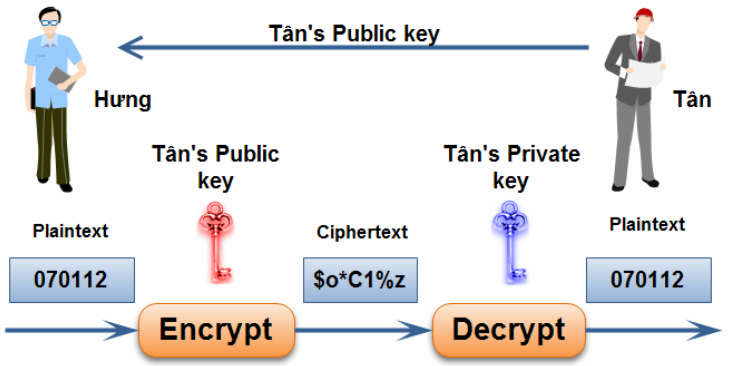
Hình A1 – 6 : Public Key Confidentiality

Vì Private key là key dùng để decrypted và đảm bảo tính bí mật, nên việc giữ cho Private key được an toàn là điều quan trọng. Nếu bất kỳ ai có được Private key của người dùng thì hoàn toàn có thể đọc được thông tin đã được encrypted bằng Public key của người dùng đó.

Public key thì có thể công bố cho mọi người mà không cần đảm bảo tính bí mật.

Cơ chế này thường được dùng để trao đổi key trong môi trường untrust (Vận chuyển Private key của thuật toán mã hóa đồng bộ).

❖ Quy tắc hoạt động



Hình A1 – 7 : Public Key Confidentiality Example

Bước 1 : Khi Tân yêu cầu Hưng gửi MSSV = "070112" qua đường Internet và phải đảm bảo tính bí mật, thì phía Tân sẽ khởi tạo bộ Public key/Private key.

Bước 2 : Tân sẽ gửi Public key của Tân cho Hưng.

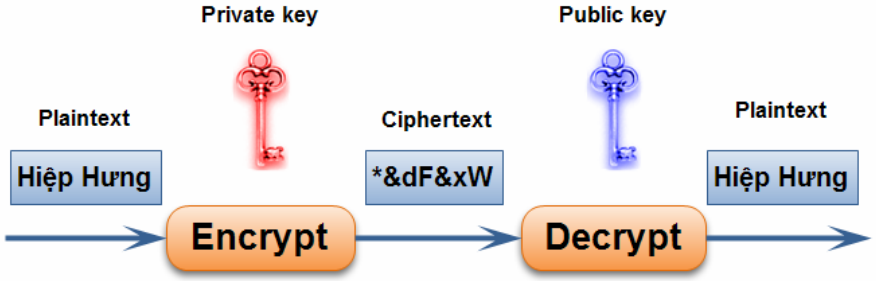
Bước 3 : Hưng sẽ sử dụng Public key của Tân để encrypted MSSV.

Bước 4 : Hưng gửi MSSV đã được encrypted thành dạng ciphertext cho Tân.

Bước 5 : Tân dùng Private key của Tân để decrypted ciphertext nhận được từ Hưng.

2.2.4.3 Public Key Authentication – Xác thực bằng Public key

Ở cơ chế này thì Private key sẽ được dùng để encrypted thông tin thành ciphertext và Public key tương ứng được dùng để decrypted ciphertext thành thông tin ban đầu.



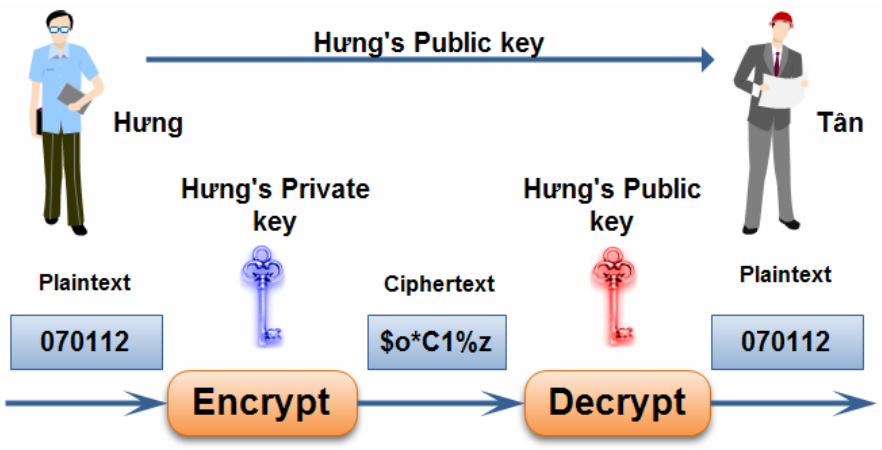
Hình A1 – 8 : Public Key Authentication

Vì Private key được dùng để encrypted và đại diện cho người dùng trong quá trình xác thực, nên phải đảm bảo tính an toàn và bí mật cho Private key. Nếu bất kỳ ai có được Private key của người dùng thì hoàn toàn có thể giả danh người dùng đó để thực hiện quá trình xác thực.

Public key thì có thể công bố cho mọi người mà không cần đảm bảo tính bí mật.

Cơ chế này thường được dùng để xác thực.

❖ Quy tắc hoạt động



Hình A1 – 9 : Public Key Authentication Example

Bước 1 : Khi Tân yêu cầu Hưng gửi MSSV = "070112" cho Tân qua đường internet và phải đảm bảo là do chính Hưng gửi, thì phía Hưng sẽ tạo bộ Public key/Private key.

Bước 2 : Hưng sử dụng Private key của Hưng để encrypted MSSV.

Bước 3 : Hưng gửi MSSV đã được encrypted thành dạng ciphertext cho Tân.

Bước 4 : Hưng gửi tiếp Public key của Hưng cho Tân.

Bước 5 : Tân dùng Public key của Hưng để decrypted ciphertext nhận được từ Hưng.

2.2.4.4 RSA Algorithm – Thuật toán RSA

RSA là thuật toán được phát minh ra bởi Rivest, Shamir, Adleman ở học viện MIT vào năm 1977 (Bản quyền hết hạn vào năm 2000).

RSA sử dụng key có chiều dài 512-2048 bits.

Thuật toán này dựa trên những điều khó khăn trong việc giải mã hiện tại là sử dụng key có chiều dài rất lớn. Như vậy thời gian giải mã sẽ vượt quá thời gian truyền dữ liệu, dù cho có giải mã được bộ key thì cũng vô dụng.

Tốc độ của RSA chậm hơn DES 100 lần ở nền hardware và 1000 lần ở nền software.

Mục đích sử dụng

- Mã hóa dữ liệu, đặc biệt cho các loại dữ liệu có kích thước nhỏ, private key của thuật toán mã hóa đồng bộ, key dùng cho HMAC.
- Dùng để xác thực.
- Tạo cơ chế Non-Repudiation.

Cơ chế tạo khóa Private key/Public key

- Chọn hai số nguyên tố **p** và **q** phân biệt
- Tính ***n=p.q***
- Tính hàm số Euler **φ(*p.q*)**=(*p*-1).(*q*-1)
- Chọn ***e*** sao cho 1<***e***<**φ(*p.q*)** và ***e*** với φ(*p.q*) là hai số nguyên tố cùng nhau – Coprime. (Chọn ***e*** là số nguyên tố sao cho **φ(*p.q*)** không chia hết cho e)
- Tính ***d*** sao cho ***de*** ≡ 1 (mod **φ(*p.q*)**) – Tức là ***de*** mod **φ(*p.q*)** = 1
- Ta có thể tính ***d*** bằng cách sử dụng biểu thức (1), tìm *x* sao cho ***d*** là số nguyên. Khi đó ta sẽ tìm được ***d***.

$$(1)\quad d = \frac{x.(q-1)(p-1)+1}{e}$$

Cơ chế encrypted/decrypted một dữ liệu ***m***

- Dữ liệu sẽ được encrypted bằng công thức $c = m^e \bmod n$ với c là chuỗi ciphertext sau khi encrypted.
- Decrypted chuỗi cipher bằng công thức $m = c^d \bmod n$
- Public key gồm ***n*** và ***e.***
- Private key gồm ***p, q*** và ***d.***

2.2.4.5 DH Algorithm – Thuật toán Diffie Hellman

DH được phát hành vào năm 1976 bởi Whitfield Diffie và Martin Hellman.

DH sử dụng key có chiều dài từ 163-1536 bits.

- Group 1 : 768bits.
- Group 2 : 1024bits (Thường được dùng).
- Group 5 : 1536bits.
- Group 7 : 163bits.

Ở RFC 3526 thì key được mở rộng thành 2048 – 3072 – 4096 – 6144 – 9192 bits.

Cũng như RSA, thì DH dựa trên những khó khăn trong việc giải mã hiện tại để tránh khóa bị giải mã.

Mục đích sử dụng

- Mã hóa dữ liệu, đặc biệt cho các loại dữ liệu có kích thước nhỏ, private key của thuật toán mã hóa đồng bộ, key dùng cho HMAC.

Cơ chế tạo khóa

- Hưng và Tân tham gia vào quá trình tạo khóa.

- Hưng và Tân sẽ thỏa thuận cặp số public gồm số nguyên tố **p** và số nguyên **g** với **g**<**p** dùng để sinh key. Với **p** là số rất lớn và **g** là số nhỏ(2, 3, 4…).
- Quy trình sinh key

Hưng	Tân
+ Hưng tạo số nguyên tố bí mật **a**.	+ Tân tạo số nguyên tố bí mật **b**.
+ Hưng tính $\mathbf{A}=\mathbf{g}^{\mathbf{a}} \bmod \mathbf{p}$	+ Tân tính $\mathbf{B}=\mathbf{g}^{\mathbf{b}} \bmod \mathbf{p}$
+ Hưng gửi **A** cho Tân và nhận **B**.	+ Tân gửi **B** cho Hưng và nhận **A**.
+ Hưng tính $\mathbf{S_H} = \mathbf{B}^{\mathbf{a}} \bmod \mathbf{p}$	+ Tân tính $\mathbf{S_T} = \mathbf{A}^{\mathbf{b}} \bmod \mathbf{p}$

- Sau giai đoạn sinh key thì
  - + Hưng sẽ có Public key là **A** và Private key là $\mathbf{S_H}$
  - + Hưng sẽ có Public key là **B** và Private key là $\mathbf{S_T}$
  - + Với $\mathbf{S_H} = \mathbf{S_T}$.

2.2.5 Digital Signature

2.2.5.1 Digital Signature Overview

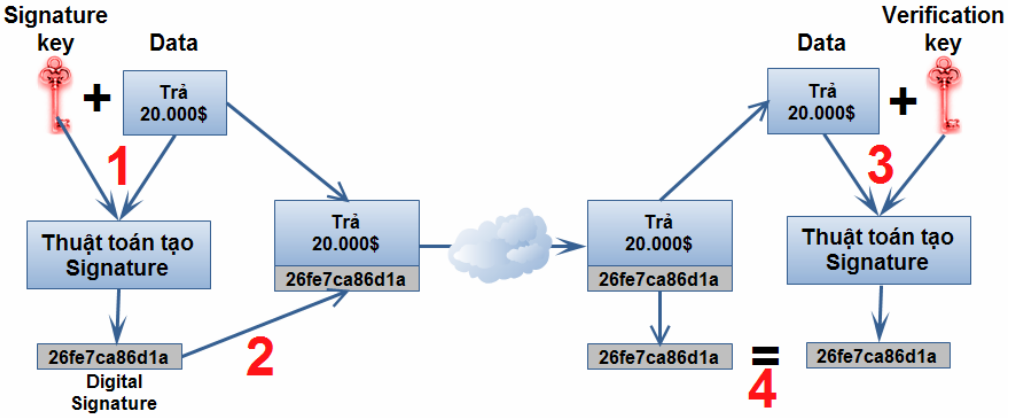
Digital Signature – Chữ ký số là thông tin đi kèm theo dữ liệu nhằm mục đích

- Data Authenticity – Xác thực dữ liệu hay xác thực người đã gửi dữ liệu.
- Data Integrity – Đảm bảo tính toàn vẹn dữ liệu.
- Non-repudiation of Transactions – Không thể chối.

Vì dữ liệu khi được truyền qua môi trường không an toàn – untrusted network thì sẽ xảy ra những vấn đề về bảo mật như

- Dữ liệu được thay đổi trong quá trình truyền tải.
- Dữ liệu nhận được từ đúng người gửi hay không.

Quy tắc hoạt động



Hình A1 – 10 : Digital Signature Example

Bước 1 : Khi người gửi cần ký vào dữ liệu của mình trước khi gửi, thì dữ liệu cùng với một Signature key (Secrect key) sẽ được đưa vào một thuật toán để tạo ra một chuỗi output được gọi là Digital Signature.

Bước 2 : Digital Signature sau đó sẽ được đính vào dữ liệu rồi gửi cho người nhận.

Bước 3 : Người nhận sẽ tách Digital Signature ra khỏi dữ liệu, đem dữ liệu cùng một Verification key cho vào thuật toán tạo Digital Signature như bên nhận.

Bước 4 : Kết quả output của bước 4 sẽ được đem so sánh với Digital Signature nhận được từ phía người gửi.

- Nếu hai kết quả giống nhau thì dữ liệu không bị thay đổi.
- Nếu hai kết quả khác nhau thì dữ liệu đã bị thay đổi khi truyền.

2.2.5.2 Đặc trưng và chức năng của DSS

DSS – Digital Signature Standard là một chuẩn Digital Signature được đưa ra bởi NIST vào năm 1994 và sử dụng thuật toán DSA – Digital Signature Algorithm để tạo Digital Signature.

Mục đích của DSS là tạo chuẩn xác thực được cho chính phủ Mỹ lúc bấy giờ.

Về sau có thêm hai thuật toán được thêm vào DSS

- RSA Digital Signature.
- ECDSA - Elliptic Curve.

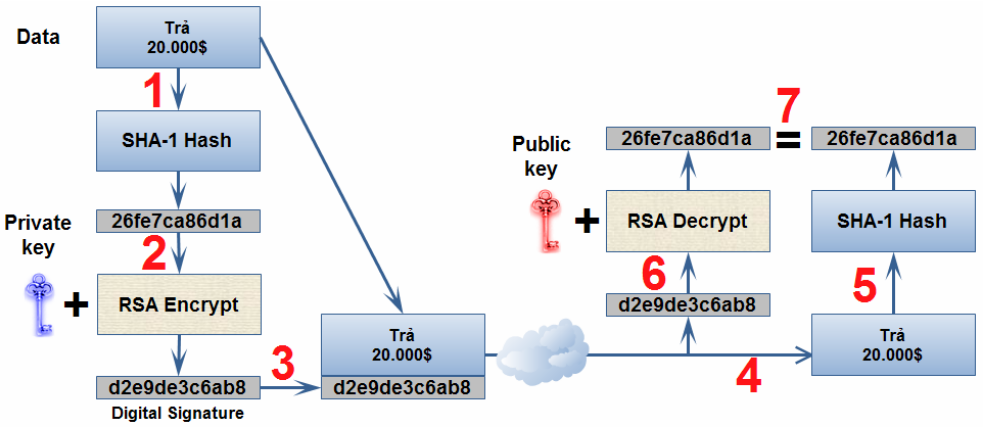
2.2.5.3 RSA Digital Signature

RSA Digital Signature là một thủ tục tạo và kiểm tra Digital Signature.

Đối với RSA Digital Signature thì quá trình tạo Digital Signature sẽ bao gồm cả thuật toán Hash và thuật toán RSA để tạo bộ Public/Private key dùng cho quá trình tạo và kiểm tra Digital Signature.

RSA Digital Signature cung cấp khả năng xác thực dữ liệu lẫn người dùng, đảm bảo tính toàn vẹn dữ liệu.

❖ Các bước tạo, sử dụng và kiểm tra chữ ký



Hình A1 – 11 : RSA Digital Signature Example

Bước 1 : Dữ liệu của người gửi sẽ được đưa vào hàm băm để lấy fingerprint.

Bước 2 : Thuật toán RSA sẽ được chạy và tính toán ra bộ Public/Private key. Fingerprint sẽ được encrypted với Private key.

Bước 3 : Phần output sau khi được encrypted là Digital Signature sẽ được đính vào dữ liệu vào gửi đi cùng với Public key được tạo từ bước 2.

Bước 4 : Phía người nhận sẽ tách Digital Signature ra khỏi dữ liệu.

Bước 5 : Phần dữ liệu sẽ được đưa vào hàm băm để lấy fingerprint_1.

Bước 6 : Phần Digital Signature sẽ được decrypted bằng Public key nhận được từ người gửi cho ra fingerprint_2.

Bước 7 : So sánh hai mẫu fingerpring_1 và fingerpring_2

- Nếu hai kết quả giống nhau thì dữ liệu không bị thay đổi.
- Nếu hai kết quả khác nhau thì dữ liệu đã bị thay đổi khi truyền.

3 Cryptanalysis

Cryptanalysis là chuyên ngành về các phương pháp giải mã và vượt qua các thuật toán mã hóa.

3.1 Bruteforce Attack

Như đã nói ở phần trên, Bruteforce Attack sẽ tấn công bằng cách thử liên tục các key có khả năng sử dụng lên một thuật toán đang hoạt động.

Tất cả các thuật toán mã hóa đều có thể bị tấn công bằng Bruteforce Attack.

Trung bình thì chỉ cần thử 50% số lượng key thì đã có thể tìm ra được key thích hợp.

Các thuật toán hiện đại được thiết kế sao cho key có độ dài lớn để thời gian giải mã thuật toán được kéo dài ra, đủ thời gian để thuật toán thực hiện xong nhiệm vụ của nó.

3.2 Ciphertext-only attack

Ở kiểu tấn công này thì hacker bắt được một số gói ciphertext, và điều cần chắc chắn là tất cả các gói này đều được encrypted bằng cùng một thuật toán.

Công việc của attacker là làm sao từ những gói ciphertext đó có thể decrypted ra được key sử dụng. Hơn thế nữa, attacker có thể suy luận ra những key có thể dùng để encrypted các ciphertext đã bắt được và đem decrypted các ciphertext khác.

Hiện tại thì cách tấn công này hầu như vô dụng bởi vì các thuật toán hiện đại đã có cơ chế phòng chống kiểu tấn công này bằng cách tạo ra các gói cipher giả được encrypted với key giả một cách ngẫu nhiên.

3.3 Known-Plaintext attack

Với kiểu tấn công này thì hacker đã biết được phần nào plaintext cũng như bắt được các gói ciphertext. Như vậy hacker sẽ dễ biết được đâu là key chính xác để lọc ra được key một cách nhanh chóng.

Tuy nhiên cũng như kiểu Bruteforce attack, thì trung bình hacker cũng phải thử 50% số lượng key trong key space mới có thể tìm ra được key chính xác.

3.4 Chosen-Plaintext attack

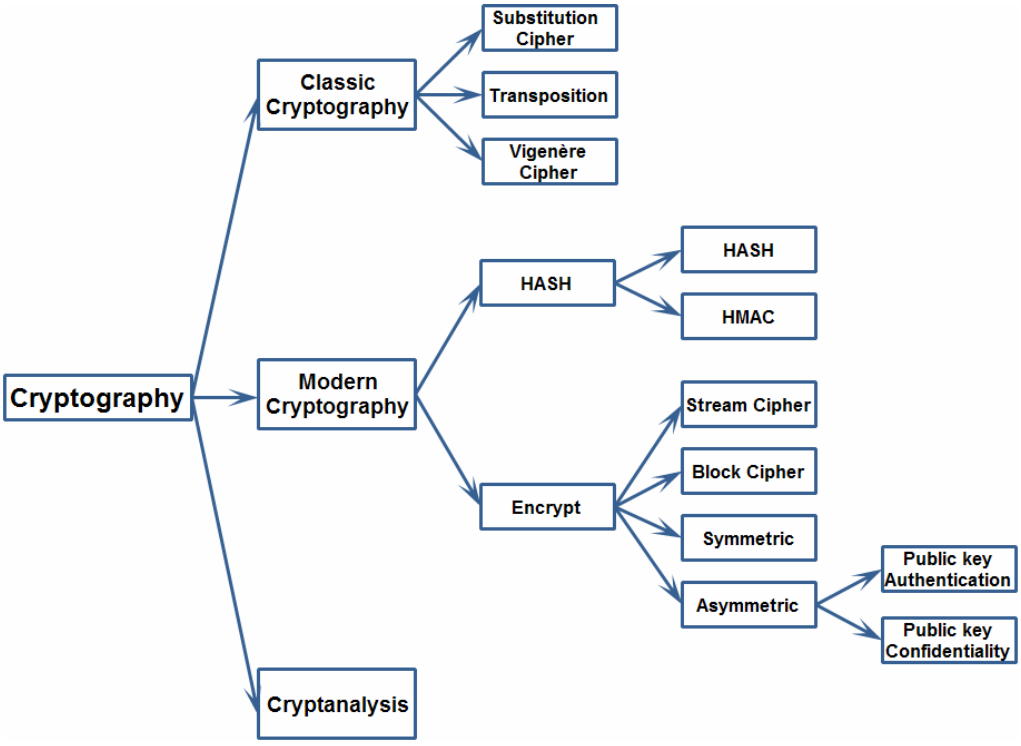
Với cách tấn công này, hack phải tiếp xúc với thiết bị encrypted và tạo ra một chuỗi plaintext để thiết bị đó encrypted chuỗi plaintext rồi bắt lại các gói cipher.

Với kiểu tấn công này thì hacker biết được thông tin nhiều hơn kiểu Known-Plaintext attack vì hacker đã trực tiếp tạo ra chuỗi plaintext nên hacker sẽ biết thêm nhiều thông tin hơn về key được sử dụng. Cách tấn công này không được hiệu quả vì việc tiếp cận thiết bị encrypted là điều rất khó.

3.5 Chosen-Ciphertext attack

Đây là kiểu tấn công giống như Chosen-Plaintext attack, nhưng thay vì tiếp cận thiết bị encrypted thì hacker tiếp cận thiết bị decrypted.

4 Cryptography Overview Chart

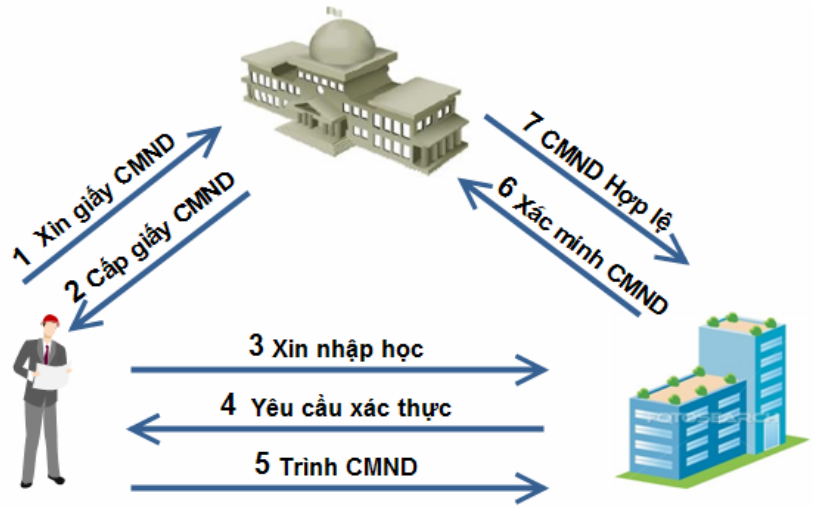


Hình A1 – 12 : Cryptography Overview Chart

5 PKI – Public Key Infrastructure

5.1 Trusted Third-Party Protocol

Trong thực tế, việc xác thực trong môi trường rộng lớp với nhiều đối tượng là điều rất khó nếu mỗi đối tượng phải xác thực tất cả đối tượng còn lại. Vì với n đối tượng thì sẽ có n.(n-1) lần xác thực. Từ đó nảy sinh ra Third-party protocol sẽ giúp đối tượng xác thực lẫn nhau một cách hiệu quả, nhanh chóng và chính xác.



Hình A1 – 13 : Trusted Third-Party

Giả sử Tân cần đăng ký vào Hoa Sen học, thì việc đầu tiên trường Hoa Sen sẽ xác nhận xem Tân có phải là công dân Việt Nam nhưng đúng quy định hay không. Việc xác nhận đó có thể được hiện thông qua giấy Chứng minh nhân dân của Tân. Bởi vì Tân đã được xác nhận bởi Công an (đươc xem như Third-party) là Công dân Việt Nam bằng xác cấp giấy Chứng minh nhân dân. Nên trường Hoa Sen chỉ cần kiểm tra giấy Chứng minh nhân dân của Tân có hợp lệ không là đủ.

Thông qua ví dụ trên thì Tân và trường Hoa Sen chính là hai đối tượng muốn xác thực lẫn nhau trong khi Công an là Third-party. Nếu cả Tân và trường Hoa Sen đều tin vào Công an thì cả hai cũng sẽ tin vào giấy Chứng minh nhân dân của Công an cấp.

5.2 PKI overview

PKI là cơ chế cho phép một bên thứ ba (Third-party) cung cấp các dịch vụ liên quan tới việc sử dụng và trao đổi Public key như

- Authenticity
- Confidentiality
- Integrity
- Non-repudiation

5.2.1 Thuật ngữ

PKI – Public Key Infrastructure là một framework cần có để hỗ trợ cho việc trao đổi, sử dụng và xác thực Public key trong hệ thống mạng.

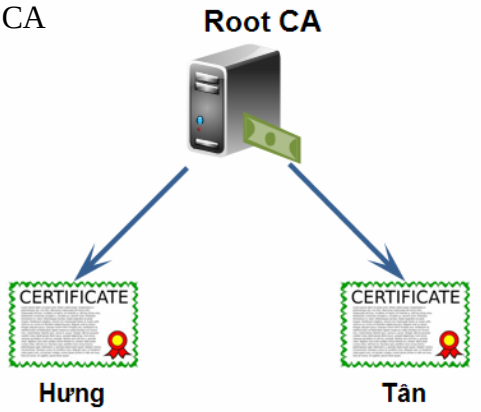
Certificate – Chứng chỉ : Tài liệu thể hiện mối ràng buộc của tên một đối tượng vào Public key của đối tượng đó và đã được ký xác nhận bởi CA. Mỗi certificate phải là độc nhất – unique ở mỗi CA domain.

CA – Certificate Authority là nơi tiếp nhận các yêu cầu tạo certificate cũng như ký xác nhận vào certificate. Tất cả các đối tượng trong hệ thống cần phải tin tưởng vào CA.

5.2.2 PKI Topologies

PKI có 3 dạng topology chính là Single Root CA, Hierarchical CAs và Cross-Certified CAs.

5.2.2.1 Single Root CA



Hình A1 – 14 : Single Root CA

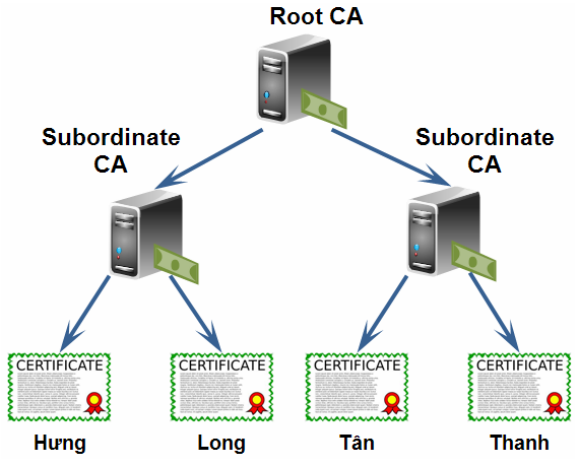
Single Root CA là dạng topology trong đó chỉ duy nhất một CA sẽ cấp certificate cho tất cả người dụng trong mạng.

Ưu điểm của dạng này là việc dựng và cài đặt dễ dàng. Tuy nhiên lại có nhiều nhược điểm đi kèm theo.

- Khó có thể mở rộng.
- Single point of failure.
- Tất cả người dùng phải tin tưởng vào CA duy nhất này, nên nếu CA này bị tấn công thì sẽ ảnh hưởng tất cả người dùng trong mạng.

5.2.2.2 Hierarchical CA

Hierarchical CA là dạng kiến trúc phân tầng với nhiều CA khác nhau bao gồm Root CA và các Subordinate CA (CA cấp dưới).



Hình A1 – 15 : Hierarchical CA

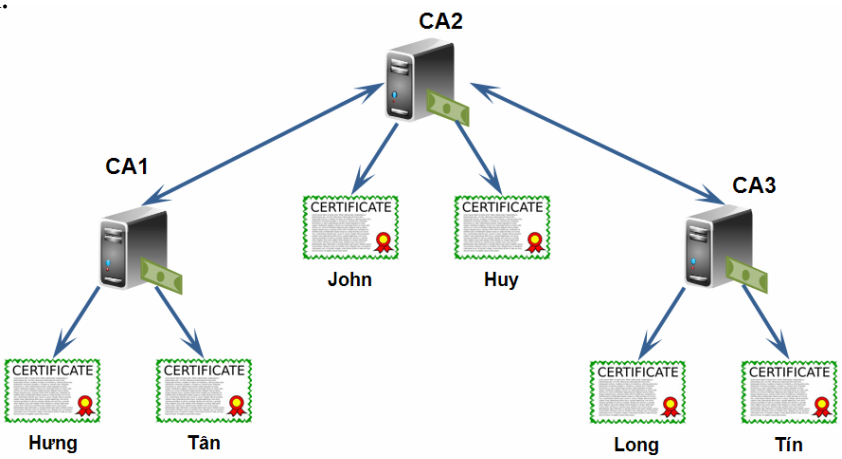
Khi một certificate được cấp thì certificate đó được gửi tới người dùng lẫn các Subordinate CA.

Với dạng kiến trúc phần tầng này, thì việc mở rộng và quản lý sẽ dễ dàng hơn. Tính tin tưởng vào CA sẽ được phân đều ra.

Thực tế ở các công ty lớn thì sẽ có một root CA và nhiều subordinate CA. Các subordinate sẽ nhận các yêu cầu đăng ký certificate từ người dùng, sau đó các yêu cầu này sẽ được gửi lên root CA để chờ root CA ký. Với cách tổ chức như vậy thì nếu subordinate CA bị mất Private key thì chỉ riêng subordinate CA đó không còn sự tin tưởng, còn các CA khác vẫn hoạt động bình thường.

5.2.2.3 Cross-Certified CAs

Đây là một dạng kiến trúc mà các CA sẽ thiết lập sự tin tưởng thông qua một CA trung gian.



Hình A1 – 16 : Cross-Certified CAs

Như trong hình thì CA1 muốn tạo mối tin tưởng với CA3 thì phải có hai yêu cầu

- CA1 phải tin CA2 và ngược lại.
- CA2 phải tin CA2 và ngược lại.

5.2.3 PKI standard

Chuẩn hóa và có khả năng tương tác cao là yêu cầu hàng đầu trong hạ tầng PKI với nhiều hãng sản xuất khác nhau. Đã có nhiều nỗ lực chuẩn hóa thành công PKI như PKCS, X.509, LDAP.

Tổ chức IETF đã thành lập các nhóm làm việc nhằm mục đích thúc đẩy sự phát triển của PKI trên nền tảng chuẩn X.509.

5.2.3.1 X.509v3

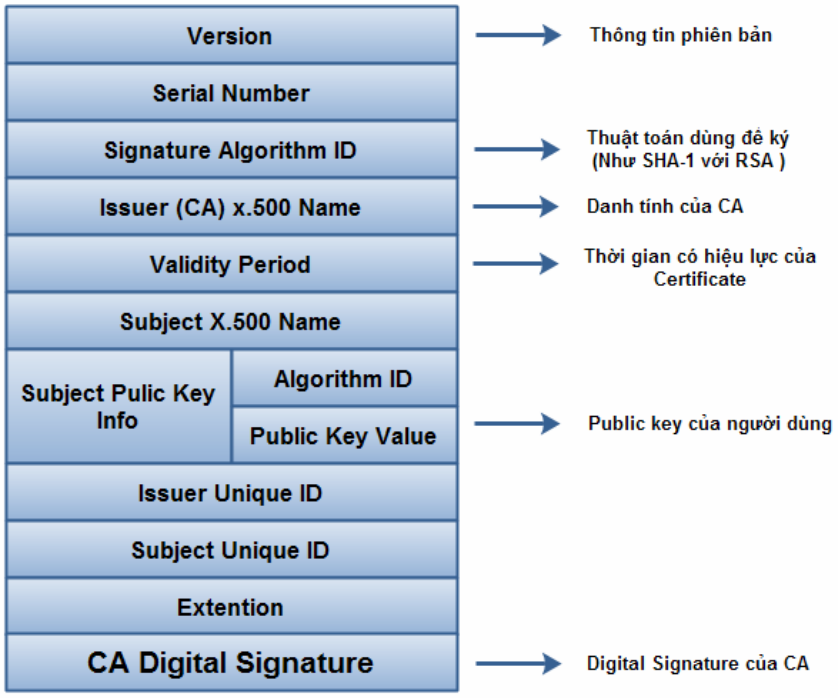
Đây là một chuẩn mô tả về cấu trúc của certificate, được dùng rộng rãi ở mọi nơi ngay cả ở môi trường internet. X509v3 thường gặp ở

- Xác thực trong giao thức SSL và TLS.
- Sử dụng trong Secure/Multipurpose Internet Mail Extention S/MIME.
- Sử dụng trong IPsec VPN.

Một ví dụ về certificate chuẩn X509v3 (Nguồn wiki).

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:68:75:47:a2:aa:c2:da:
                   84:25:fc:a8:f4:47:51:da:85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:
                   06:6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:6a:0c:44:38:cd:fe:
                   be:e3:64:09:70:c5:fe:b1:6b:29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:
                   e7:90:6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:5d:c3:58:e1:c0:
                   e4:d9:5b:b0:b8:dc:b4:7b:df:36:3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
  Signature Algorithm: md5WithRSAEncryption
      07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:a8:6f:49:1a:e6:da:51:e3:6
      0:70:6c:84:61:11:a1:1a:c8:48:3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd
      :88:4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:8a:6f:9a:29:9b:99:18:
      28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a
      9:da:b9:b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:70:47
```

Cấu trúc chung certificate chuẩn X509v3



Hình A1 – 17 : Certificate Structure

5.2.3.2 PKCS

PKCS – Public-Key Cryptographic Standard là tiêu chuẩn được đề ra bởi RSA Security. Mục đích của PKCS là chuẩn hóa các công nghệ về Public key.

5.2.4 Certificate Authority - CA

Các công nghệ về Public key ngày càng được sử dụng rộng rãi ở nhiều lĩnh vực khác nhau và dần trở thành tiêu chuẩn cơ bản của việc bảo mật. Từ đó dẫn đến việc cần phải có một trung tâm quản lý các Public key này cũng như phải có một giao thức để giúp việc trao đổi Public key được an toàn và tin tưởng. Các Public key sẽ được một trung tâm quản lý cấp giấy phép – certificate để có thể được sử dụng trong hạ tầng PKI. Các certificate này sẽ đại diện cho một người dùng, thiết bị, server… Như vậy việc quản lý các Public key trở thành việc quản lý các certificate.

CA được xem như là một điểm được tin tưởng ở trong hạ tầng PKI có nhiệm vụ nhận các yêu cầu tạo certificate, ký, phân phối, thu hồi và hủy certificate.

Sử dụng CA sẽ giúp việc quản lý key trở nên tập trung hơn thông qua việc tạo mối ràng buộc giữa những danh tính của người dùng vào Public key của họ để tạo thành certificate.

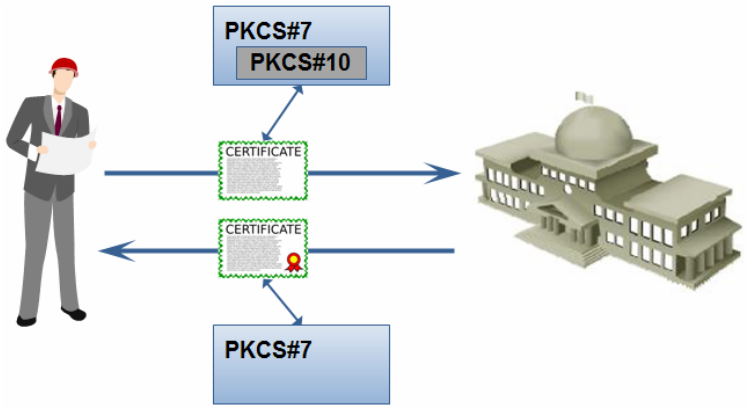
Trước khi hạ tầng PKI có thể hoạt động thì CA sẽ tạo ra bộ Public/Private của riêng CA. Sau đó tạo ra một certificate cho chính CA rồi tự ký vào certificate đó.

Certificate của CA sẽ chứa những thông tin liên quan tới CA

- Danh tính của CA.
- Số seri, thuật toán sử dụng, thời gian hết hạn.
- Public key của CA (được tạo bằng thuật toán như RSA).
- Digital Signature – Phần chữ ký số tự CA ký vào Certificate của CA bằng Private key.

Cách tổ chức của CA bao gồm Single Root CA, Hierarchical CAs và Cross-Certified CA như đã nêu ở phần **2.2.**

5.2.4.1 Simple Certificate Enrollment Protocol



Hình A1 – 18 : Simple Certificate Enrollment Protocol

SCEP là giao thức hỗ trợ cho CA và người dùng có thể đăng ký và thu hồi certificate một cách tự động mà vẫn đảm bảo được tính an toàn về dữ liệu.

Người dùng sẽ tạo một yêu cầu tạo certificate bằng chuẩn PKCS#10, sau đó gửi đi bằng chuẩn PKCS#7.

Khi CA hoặc RA (Registration Authority) nhận đưcợc yêu cầu sẽ xác thực người dùng. Nếu xác thực thành công thì CA sẽ ký vào Certificate rồi gửi trả về cho người dùng bằng chuẩn PKCS#7.

5.2.4.2 Quá trình lấy Certificate của CA

Đây là quá trình người dùng xác thực CA và đảm bảo đây là CA đáng tin tưởng.

Người dùng sẽ lấy Certificate của CA (thường là bằng inband).

Người dùng sẽ xác thực Certificate bằng các thuật toán cùng Public key có trong Certificate, sử dụng điện thoại để liên hệ với CA Administrator (Out-of-band).

5.2.4.3 Quá trình gửi yêu cầu

Sau khi xác thực Certificate là hợp lệ và chính xác của CA, thì người dùng sẽ tạo một request xin certificate.

Request đó chứa các thông tin đủ để tao ra một certificate như tên,thông tin cá nhân, thông tin công ty và quan trọng nhất là Publickey của người dùng.

Tất cả các thông tin đó được encrypted bằng Public Key của CA.

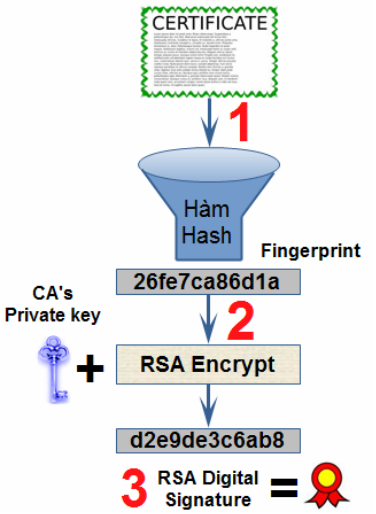
Request được tạo sẽ gửi đến CA (Inband).

5.2.4.4 Quá trình ký vào Certificate

Khi CA nhận được một request xin certificate thì CA sẽ tiến hành xác thực người dùng bằng điện thoại với những thông tin cần thiết (Out-of-band).

Khi xác thực thành công thì CA sẽ tiến hành ký vào Certificate.

❖ Quá trình ký vào Certificate (RSA Digital Signature)



Bước 1 : Những thông tin của người dùng sẽ được tổng hợp lại thành một Certificate. Certificate đó được đưa vào hàm hash SHA-1. Kết quả cho ra Fingerprint.

Bước 2 : Fingerprint sẽ được encrypted bằng thuật toán RSA với Private key của CA để tạo ra Digital Signature.

Bước 3 : Digital Signature được đính vào Certificate ở bước 1 để tạo ra một Certificate hoàn chỉnh đã được ký.

Hình A1 – 19 : Certificate Signing

5.2.4.5 Hoàn tất thủ tục xin Certificate

Sau khi certificate được tạo và ký bởi CA, certificate sẽ được trả cho người dùng.

Người dùng có thể lấy certificate được trả về từ CA bằng nhiều các khác nhau

- Vào website của CA lấy trực tiếp (Inband).
- Vào website của CA và xác thực bằng tài khoản để lấy (Out-of-band).
- CA gửi thư về cho người dùng (Out-of-band).
- Người dùng lên trực tiếp trụ sở của CA lấy (Out-of-band).

5.2.4.6 Xác thực người dùng bằng Certificate

Khi muốn xác thực người dùng bằng Certificate thì điều cần có là Public key của CA có trong Certificate của CA.

Certificate của CA có thể lấy được bằng mục **2.2.1** hoặc đã được tích hợp sẵn trong hệ điều hành, trình duyệt và được thường quyên cập nhật thông qua các bản vá.

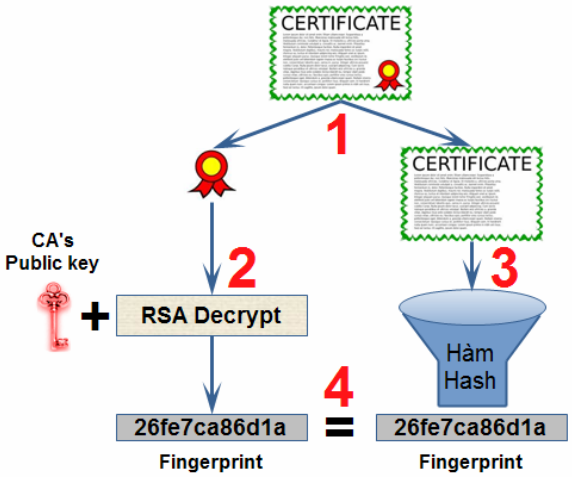
❖ Các bước xác thực

Bước 1 : Khi có được Certificate của người gửi, thì người nhận sẽ tách Certificate ra làm hai phần là Digital Signature và Certificate không có chữ ký.

Bước 2 : Phần Digital Signature sẽ được decrypted bằng thuật toán RSA với Public key của CA(có được từ Certificate của CA). Kết qua ra chuỗi fingerprint.

Bước 3 : Phần Certificate không chữ ký sẽ được đưa qua hàm hash SHA-1. Kết quả cho ra chuỗi fingerprint.

Bước 4 : So sánh hai chuỗi fingerprint ở bước 2 và bước 3. Nếu giống nhau thì Certificate của người gửi hợp lệ.



Hình A1 – 20 : Certificate Verification

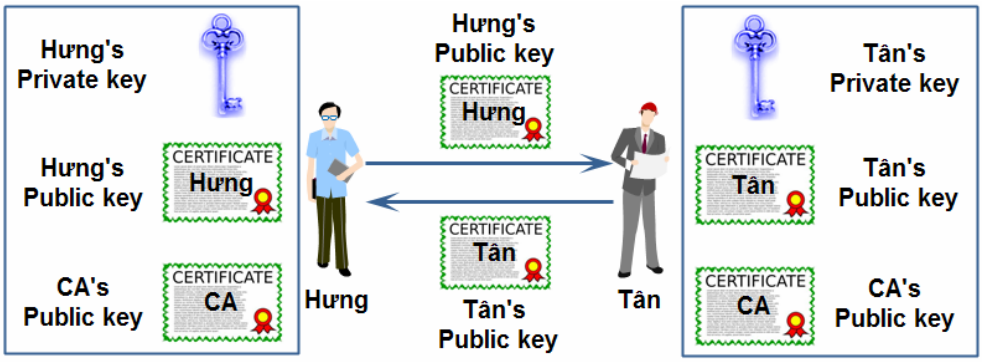
❖ Nhận xét

Trong các bước vừa nêu, ta có thể thấy vai trò của Private key của CA hết sức quan trọng. Private key của CA đảm bảo rằng chuỗi hash của certificate sẽ được mã hóa an toàn, đồng thời cũng là yếu tố tham gia vào quá trình xác thực (Private key để encrypted và Public key để decrypted).

Cho nên việc giữ cho Private key của CA được bí mật và an toàn là điều rất quan trọng. Việc CA mất Private key cũng đồng nghĩa CA đó không còn đủ tin tưởng và trở nên vô dụng trong hạ tầng PKI.

5.2.4.7 Ví dụ thực tế

Hưng và Tân cần thiết lập một kết nối an toàn sử dụng thuật toán mã hóa đồng bộ AES. Nhưng điều trở ngại lớn nhất ở đây là làm sao Hưng và Tân trao đổi Share Secret key cho nhau được an toàn và làm sao xác thực được lẫn nhau.



Hình A1 – 21 : Example

- Hưng/Tân lấy certificate của CA về.
- Hưng/Tân tiến hành việc kiểm tra tính hợp lệ của certificate của CA.
- Hưng/ Tân tạo bộ Public/Private key bằng thuật toán RSA.
- Hưng/Tân gửi Public key cùng những thông tin cá nhân đã được encrypted bằng Public key của CA lên cho CA.
- CA tạo certificate cho Hưng/Tân rồi ký vào certificate đó như phần 2.4.4.
- Certificate đã ký được gửi về cho Hưng/Tân.
- Khi Hưng muốn tạo kết nối an toàn bằng thuật toán mã hóa đồng bộ AES thì Hưng sẽ tạo ra Share Secret key cho thuật toán AES.
- Tân gửi Certificate của Tân đến cho Hưng.
- Hưng sẽ dùng Public key của CA để xác thực certificate của Tân như phần 2.4.6.
- Nếu xác thực chính xác đây là certificate của Tân thì Hưng sẽ dùng Public key của Tân có trong Certificate vừa nhận để encrypted Share Secret key ra chuỗi ciphetext rồi gửi phần ciphertext đó cho Tân.
- Tân nhận được phần ciphertext sẽ lấy Private key của Tân để decrypted.

- Như vậy Hưng đã gửi thành công Share Secret key cho Tân một cách an toàn và bí mật.

5.2.5 Server Offload

CA cùng Private key của nó là thành phần cần được bảo vệ nhiều nhất trong hạ tầng PKI. Để đảm bảo hoạt động của CA được đơn giản và an toàn thì việc quản lý key sẽ được giao phó cho Registration Authorities (RAs).

Registration Authorities sẽ đảm nhận các nhiệm vụ

- Xác thực người dùng đăng ký Certificate.
- Quản lý việc tạo key của người dùng trong trường hợp cần.
- Phân phối Certificate.
- Chịu trách nhiệm như một proxy tới CA.
- Giảm thiểu tối đa sự xuất hiện của CA đối với người dùng.

Từ đó, nhiệm vụ của CA chỉ là ký vào các certificate thay vì đảm nhận nhiều công việc như trước.

B . IPsec VPN

1 VPN Overview

1.1 History

Trước những năm 1990, việc kết nối hai vùng Private, hai chi nhánh của cùng một công ty ở hai khu vực cách xa nhau về mặt địa lý là rất đắt tiền. Hai phương pháp thường dùng là Leased Lines hoặc là Dial-up. Cả hai phương án đó đều có chi phí rất cao (hơn 1,000$ cho đường 56kbps và hơn 10,000$ cho đường T1, phụ thuộc vào khoảng cách giữa hai vùng).

Từ đó đặt ra cần có một giải pháp kết nối các vùng Private lại với nhau với chi phí thấp, đạt hiệu quả về kinh tế cũng như về hiệu suất hoạt động.

1.2 Virtual Private Network - VPN

VPN là một phương thức truyền thông sử dụng hạ tầng viễn thông công cộng như Internet để kết nối các vùng Private (các cá nhân, tổ chức, các chi nhánh của cùng một công ty…) lại với nhau với chi phí thấp và có hiệu suất truyền tải cao.

VPN sẽ tạo một kết nối ảo – Tunnel giữa các vùng Private, gói tin đi trong đường kết nối ảo đó sẽ được đóng gói – Encapsulation với các chuẩn VPN khác nhau.

Ban đầu VPN ra đời chỉ mục đích là kết nối các vùng Private, nhưng về sau do những thông tin được truyền có nguy cơ bị lộ cùng với sự phát triển của Hackers, cho nên VPN đã được xây dựng cùng với các thuật toán bảo mật (Encryption, HASH…). Về sau này, VPN mặc định là có các thuật toán bảo mật để bảo vệ dữ liệu được truyền.

Có hai dạng VPN thường gặp là Site-to-Site và Remote Access.

Site-to-Site là dạng kết nối chữa hai hay nhiều Gateway, tạo đường kết nối ảo cho các mạng Private.

Remote Access là tạo đường kết nối giữa người dùng từ xa tới Gateway.

1.3 Benefits of VPN

Những lợi ích có được khi sử dụng VPN là tiết kiệm chi phí, tăng tính bảo mật, có khả năng mở rộng cao.

- Tiết kiệm chi phí – Cost Saving

  Sử dụng VPN sẽ giúp tiết kiệm tối đa chi phí thay vì phải thuê đường truyền từ các nhà cung cấp dịch vụ thứ ba (Leased Line, Post office…).

  Băng thông đường truyền VPN cao hơn băng thông Leased Line hay Dial-up.

- Bảo mật – Security

  VPN cung cấp khả năng mã hóa và xác thực dữ liệu, nên dữ liệu truyền trên đường VPN sẽ được đảm bảo tính bí mật và không có khả năng giả mạo dữ liệu.

- Khả năng mở rộng cao – Scalability

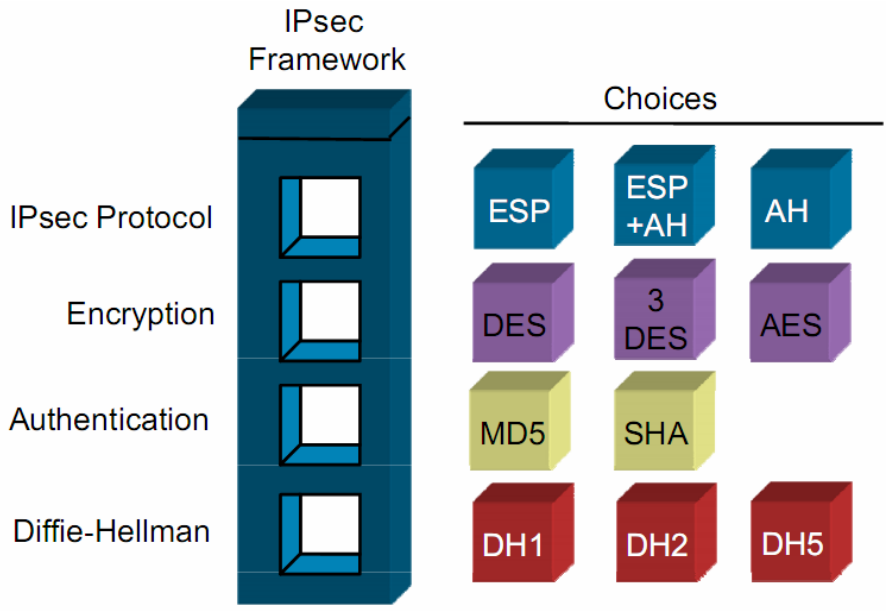
  Do VPN sử dụng hạ tầng mạng Internet, cho nên việc mở rộng thêm một vùng Private tham gia vào hệ thống VPN có sẵn là rất dễ dàng, không cần trang bị thêm thiết bị hay dịch vụ nào khác nữa.

2 IPsec VPN

IPsec là chuẩn VPN làm việc ở lớp Network (IP protocol), giúp bảo vệ và xác thực các gói tin được truyền giữa hai thiết bị IPsec (peers).

IPsec không phải là giao thức mã hóa, xác thực hay bảo vệ dữ liệu, IPsec là một khuôn mẫu – Framework tập hợp các thuật toán giúp mã hóa, xác thực và bảo vệ dữ liệu.

IPsec tạo đường kết nối giữa host với host, host với Gateway và Gateway với Gateway.



Hình A2 – 1 : IPsec Framework

2.1 Workflow

Khi một kết nối được tạo từ host A tới host B thì sẽ trải qua các bước như sau

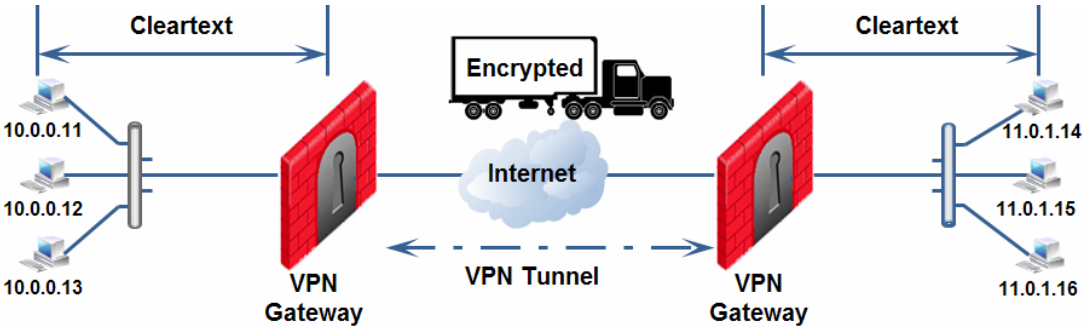
Bước 1 : Kết nối được tạo từ host A sẽ đi tới Gateway 1, các gói đi giữa host A tới Gateway vẫn là dạng cleartext.

Bước 2 : Gateway 1 nhận kết nối và kiểm tra địa chỉ Source và Destination để quyết định kết nối này có sử dụng VPN hay không.

Bước 3 : Nếu là lần đầu tiên Gateway 1 và Gateway 2 giao tiếp với nhau thì giữa hai Gateway sẽ khởi tạo các bước đàm phán IKE – Internet Key Exchange để tạo kết nối VPN.

Bước 4 : Sau khi kết nối VPN được tạo, Gateway 1 encrypted các dữ liệu đến từ host A rồi gửi đi. Như vậy dữ liệu đi giữa hai Gateway của host A đi tới host B là ciphertext.

Bước 5 : Khi Gateway 2 nhận được các dữ liệu từ Gateway 1, Gateway 2 sẽ decrypted các dữ liệu đó, kiểm tra Source và Destination của các gói tin rồi chuyển chính xác tới đích cần tới (ở đây là host B). Dữ liệu từ Gateway đến host B là Cleartext.



Hình A2 – 2 : IPsec Site-to-Site VPN Workflow

2.2 IPsec Functions

IPsec cung cấp khả năng bảo vệ, xác thực và đảm bảo tính toàn vẹn dữ liệu.

❖ Tính bí mật – Data confidentiality

Dữ liệu đi giữa đường IPsec VPN sẽ được encrypted bằng những thuật toán để đảm bảo dữ liệu không thể bị đọc được nếu có người bắt được gói tin.

Các thuật toán thường được sử dụng : AES, DES, 3DES.

❖ Đảm bảo toàn vẹn dữ liệu – Data Integrity

Dữ liệu khi đi bằng đường IPsec VPN sẽ được đảm bảo tính toàn vẹn.

Nếu bất kỳ dữ liệu nào bị phát hiện là đã bị thay đổi thì dữ liệu đó sẽ bị từ chối.

Hai thuật toán Hash được sử dụng để đảm bảo tính toàn vẹn dữ liệu là HMAC-MD5 và HMAC-SHA1.

❖ Xác thực nguồn gửi – Origin Authentication

Đảm bảo các Peers tạo kết nối là chính xác và tin tưởng. Đồng thời dữ liệu được gửi chính xác từ Peers mong muốn.

Hai cách xác thực nguồn gửi thường dùng là Pre-shared Key và Digital Signature.

2.3 IPsec Security Protocol

2.3.1 Tunnel Mode và Transport Mode

2.3.1.1 Transport

Trong Transport Mode thì phần IPsec Header (AH hoặc ESP Header) sẽ được chèn vào giữa IP Header và phần Data (bao gồm Layer 4 Data và Layer 4 Header).

Trong chế độ này thì IP Header của gói tin AH sẽ giống với IP Header của gói tin gốc ngoại trừ phần "IP Header checksum" và trường "IP Protocol" là bị thay đổi.

- IP Protocol = 50 với ESP
- IP Protocol = 51 với AH

Khi dùng chế độ này thì IPsec sẽ giả định rằng hai Endpoint đi đến nhau – Reachable, nên Source IP và Destination IP của gói tin IPsec sẽ không bị thay đổi. Như

vậy chế độ Transport Mode chỉ sử dụng khi Endpoint và VPN Gateway cùng là một thiết bị.

AH thường được dùng trong trường hợp hai host giao tiếp trực tiếp với nhau, như vậy hai host đó phải được route trong suốt quãng đường đi giữa hai host (Do gói tin AH sẽ không được NAT).

2.3.1.2 Tunnel Mode

Trong Tunnel Mode thì toàn bộ gói tin ở Layer 3 (IP packet) sẽ được đóng gói thành một IP packet mới và IPsec Header (AH hoặc ESP Header) sẽ được chèn giữa IP header của gói tin gốc và IP header mới.

Tunnel Mode thường được dùng cho các host giao tiếp với nhau thông qua các VPN Gateway hoặc giữa host với VPN Gateway.

2.3.2 Authentication Header – AH

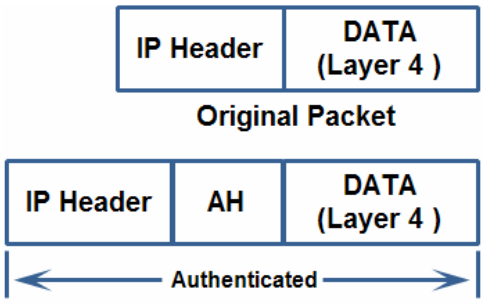
Giao thức AH cung cấp khả năng xác thực và đảm bảo tính toàn vẹn dữ liệu.

Giao thức AH đảm bảo tính toàn vẹn dữ liệu cho cả IP Header của gói tin.

Tuy nhiên AH lại không cung cấp khả năng mã hóa dữ liệu. Như vậy dữ liệu truyền giữa các Gateway là cleartext, cho nên nếu gói tin bị bắt trên đường đi thì hacker vẫn có thể đọc được thông tin có trong gói tin AH.

AH sử dụng phương pháp chèn (Insert) header vào gói tin IP packet gốc.

2.3.2.1 AH Transport Mode

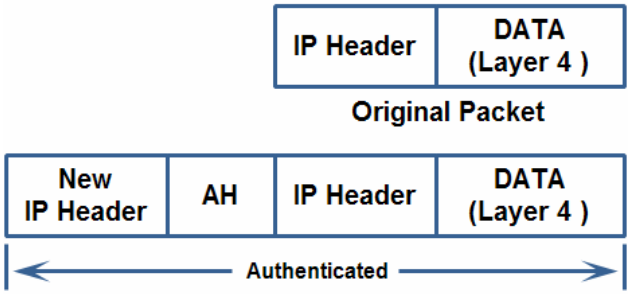


Hình A2 – 3 : AH Transport Mode Packet

Trong AH Tranport Mode thì gói tin gốc sẽ được chèn thêm AH Header vào.

Quá trình xác thực gói tin AH bao gồm IP Header và Data.

2.3.2.2 AH Tunnel Mode



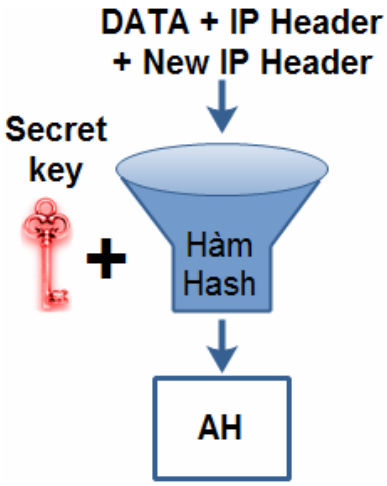
Hình A2 – 4 : AH Tunnel Mode Packet

Trong AH Tranport Mode thì gói tin gốc sẽ được đóng gói thành một IP packet mới với IP Header mới, AH Header được chèn vào giữa IP Header và New IP Header.

Quá trình xác thực gói tin AH bao gồm IP Header, Data và New IP Header.

2.3.2.3 AH Authentication and Integrity

Quá trình xác thực và đảm bảo tính toàn vẹn dữ liệu dựa vào các thuật toán HMAC (MD5 hoặc SHA-1).



Bước 1 : IP Header, Data và New IP Header (nếu có) sẽ được đưa vào hàm Hash cùng với Secret Key.

Bước 2 : Giá trị Hash được đưa vào AH Header.

Bước 3 : AH Header được chèn vào IP Packet.

Bước 4 : Gói tin được gửi đến Destination.

Bước 5 : Destination sẽ thực hiện lại hàm Hash bao gồm IP Header, Data, New IP Header (nếu có).

Bước 6 : Giá trị Hash ở Source và Destination sẽ được đem so sánh. Nếu giống thì nguồn gửi là chính xác và dữ liệu không bị thay đổi trong quá trình truyền gửi.

Hình A2 – 5 : AH Authentication and Integrity

2.3.3 Encapsulating Security Payload – ESP

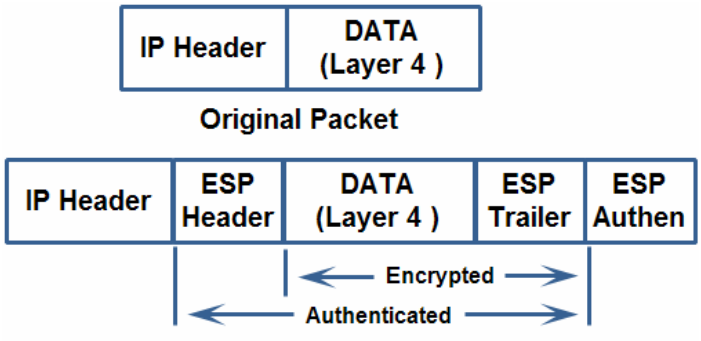
Giao thức ESP cung cấp khả năng xác thực, bảo đảm tính toàn vẹn và mã hóa dữ liệu.

ESP encrypted toàn bộ dữ liệu được gửi đi (tính từ ESP Header trở về sau), cho nên trong quá trình gửi trên Internet, gói tin không thể bị đọc được nếu hacker bắt được.

Tuy nhiên ESP không hỗ trợ xác thực IP Header hoặc New IP Header (nếu có) do chỉ xác thực dữ liệu từ ESP Header trở về sau.

ESP sử dụng phương pháp đóng gói – Encapsulation gói tin IP packet gốc.

2.3.3.1 ESP Transport Mode



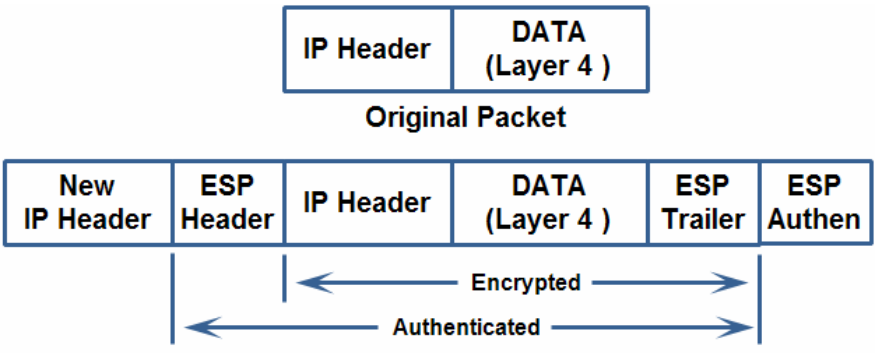
Hình A2 – 6 : ESP Tranport Mode Packet

Trong ESP Transport Mode thì phần Data sẽ được đóng gói vào trong gói tin ESP, phần IP Header gốc sẽ được giữ lại.

Quá trình mã hóa bao gồm Data và ESP Trailer.

Quá trình xác thực bao gồm Data, ESP Trailer và ESP Header.

2.3.3.2 ESP Tunnel Mode



Hình A2 – 7 : ESP Tunnel Mode Packet

Trong ESP Tunnel Mode thì phần Data và IP Header sẽ được đóng gói vào trong gói tin ESP, sau đó toàn bộ sẽ được đóng gói vào IP packet mới với New IP Header.

Quá trình mã hóa bao gồm Data, IP Header và ESP Trailer.

Quá trình xác thực bao gồm Data, IP Header, ESP Trailer và ESP Header.

2.3.3.3 ESP Authentication and Integrity

Cũng như AH, ESP cũng xác thực và đảm bảo tính toàn vẹn dữ liệu được vào các thuật toán HMAC (MD5 hoặc SHA-1).

Trong Transport Mode thì phần Data, ESP Trailer và ESP Header cùng với Secret Key được đưa vào hàm Hash.

Trong Tunnel Mode thì phần Data, IP Header, ESP Trailer và ESP Header cùng với Secret Key được đưa vào hàm Hash.

Kết quả Hash sẽ được đưa vào trường ESP Authen để xác thực và đảm bảo tính toàn vẹn dữ liệu.

Do ESP không xác thực luôn phần IP Header chính của gói tin cho nên Attacker có thể tấn công vào điểm yếu này.

2.4 Security Association – SA

SA là tập hợp các chính sách và các keys dùng trong quá trình thiết lập và bảo vệ dữ liệu truyền trong đường IPsec VPN. Có hai dạng SA

- *IKE SA hay ISAKMP SA là kết quả của IKE Phase I.*
- *IPsec SA là kết quả của IKE Phase II.*

2.4.1 IKE SA

Sau khi đàm phán thành công ở IKE Phase I, thì mỗi VPN Gateway sẽ đưa ra một SA để bảo vệ đường kết nối Inbound lẫn Outbound ở Phase II. Cả 2 SA ở hai VPN Gateway là giống nhau (Bidirectional SA), bao gồm các thông tin

- ❖ Policy set quy định
  - Thuật toán mã hóa – Encryption Algorithm
  - Thuật toán Hash – Hash Algorithm
  - Kiểu xác thực – Pre-shared Key/Digital Signature
  - Diffie – Hellman group
  - Thời gian tồn tại – Life time (Mặc định là 24h)
- ❖ Bộ key
  - Pre-shared Key
  - DH Public Key
  - SKEYID
  - SKEYID_A
  - SKEYID_E
  - SKEYID_D

2.4.2 IPsec SA

Là kết quả của quá trình đàm phán thành công của Phase II, mỗi VPN Gateway sẽ đưa ra một cặp SA (một dùng cho Inbound và một dùng cho Outbound) để bảo vệ đường truyền dữ liệu.

Nếu Gateway A và Gateway B tham gia tạo đường VPN thì

- Outbound SA của Gateway A sẽ giống Inbound SA của Gateway B.
- Inbound SA của Gateway A sẽ giống Outbound SA của Gateway B.

IPsec SA bao gồm các thông tin

- ❖ Policy set quy định
  - Thuật toán mã hóa – Encryption Algorithm.
  - Thuật toán Hash – Hash Algorithm.
  - Diffie-Hellman group (Nếu dùng PFS).
  - Thời gian tồn tại – Life time (Mặc định là 3600s hoặc 10000KB).
  - IPsec Protocol (ESP hoặc AH).
  - Mode (Tunnel hoặc Transport).
  - Local IP và Peer IP.

- ❖ Bộ key
  - Encryption Key
  - HMAC Key

2.5 Internet Key Exchange – IKE

Quá trình mã hóa dữ liệu sử dụng các thuật toán mã hóa đồng bộ - Symmetric Algorithm. Trong đó hai Gateway tham gia vào đường VPN sử dụng cùng một ShareSecrect key.

Nhưng khó khăn vả trở ngại lớn nhất làm sao trao đổi Share Secret Key của thuật toán mã hóa đồng bộ trên môi trường Internet.

IKE là một chuẩn tập hợp các phương thức, khuôn mẫu (Framework) với mục đích xác thực, tạo key và tạo kết nối an toàn, bao gồm

- ISAKMP
- Oakley
- SKEME

ISAKMP cung cấp một framework dùng để xác thực, trao đổi key nhưng không qui định key sẽ được tạo như thế nào.

Oakley mô tả các phương pháp trao đổi key (gọi là các mode) và mô tả chi tiết các dịch vụ dành cho các phương pháp đó (Perfect forward secrecy cho Key, bảo mật danh tính và xác thực).

SKEME mô tả các kỹ thuật trao đổi key linh động và cung cấp tính nặc danh, repudiability và làm mới key liên tục.

Hầu hết các hãng thiết bị thường dùng ISAKMP trong IKE nên khi nhắc đến IKE thì ngầm mặc định là ISAKMP.

IKE sử dụng ba mode để tạo môi trường truyền thông an toàn

- Main Mode dùng cho Phase I.
- Aggressive dùng cho Mode Phase I.
- Quick mode dùng cho Phase II.

Quá trình hoạt động của IPsec VPN từ lúc nhận được kết nối VPN cho tới lúc kết thúc đường VPN sẽ trải qua năm bước, trong đó có hai giai đoạn sử dụng IKE.

Step 1 : Interesting Traffic Initiates the IPsec Process.

Step 2 : IKE Phase I.

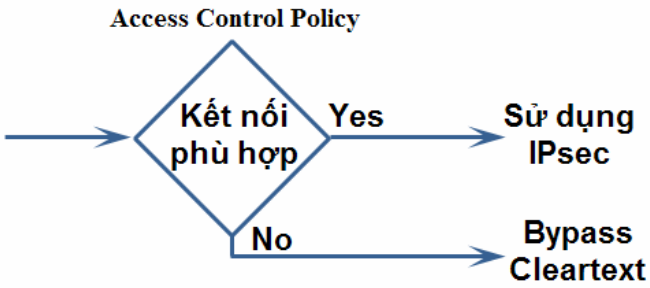
Step 3 : IKE Phase II.

Step 4 : Data Transfer.

Step 5 : IPsec Tunnel Termination.

2.5.1 Step 1 : Interesting Traffic Initiates the IPsec Process

Khi một host tạo kết nối thông qua VPN Gateway, thì VPN Gateway sẽ kiểm tra Access Control Policy và quyết định kết nối đó có đi phải được bảo vệ bằng đường IPsec VPN hay gửi đi ở dạng cleartext.



Hình A2 – 8 : Access Control Policy

Cả hai hướng Inbound và Outbound của VPN Gateways luôn có hai sự lựa chọn đối với dữ liệu là áp đặt chính sách bảo vệ của IPsec VPN (encrypted/decrypted) hoặc đi qua theo Access Control Policy (Bypass).

Chi tiết việc phân loại kết nối có hoặc không sử dụng IPsec VPN được đề cập ở mục *Access Control and VPN Communities(Phần B – I – mục 2. 7 trong cùng Chapter).*

Sau khi xác định dữ liệu cần sử dụng đường VPN, thì VPN Gateway khởi động bước tiếp theo là IKE Phase I.

2.5.2 Step 2 : IKE Phase I

Mục đích của Phase I là đàm phán bộ IKE Policy (Phase I Policy), xác thực VPN Gateway peer và thiết lập đường kết nối an toàn giữa VPN Gateway peers để chuẩn bị cho IKE Phase II.

Kết quả sau khi đàm phán IKE Phase I là bộ IKE SA.

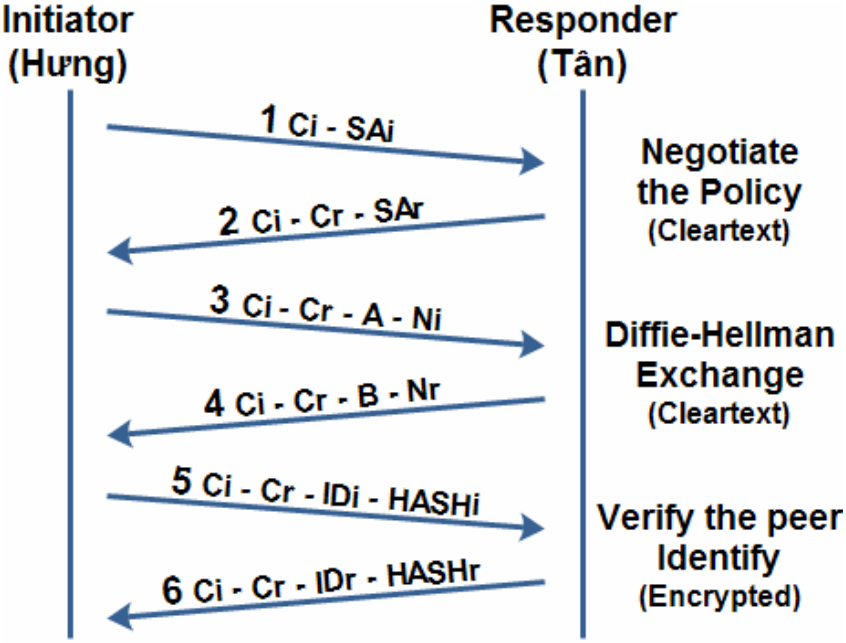
IKE Phase I có thể chạy ở Main Mode hoặc Aggressive Mode.

2.5.2.1 Main Mode

Quá trình hoạt động của IKE Phase I Main Mode chia làm 3 bước nhỏ, mỗi bước sử dụng 2 gói tin để hoạt động. Như vậy tổng cộng có 6 gói tin ở Main Mode.

- Step 2-1 : Negotiate the Policy.
- Step 2-2 : Diffie-Hellman Exchange.
- Step 2-3 : Verify the peer Identify.

Phía khởi tạo kết nối IPsec VPN là Initiator, phía còn lại nhận kết nối IPsec VPN là Responder.



Hình A2 – 9 : Main Mode Workflow

❖ Step 2-1 : Negotiate the Policy

Ở *gói tin thứ nhất*, Initiator sẽ gửi cho Responder chuỗi Cookie **Ci** cùng với bộ Policy **SAi** (Quy định các thuật toán mã hóa, Hash, phương thức xác thực…).

Phía Responder nếu tìm được bộ Policy phù hợp **SAr** với phía Initiator, thì ở *gói tin thứ hai*, Responder sẽ gửi về cho Initiator chuỗi Cookie **Cr** cùng **SAr**.

Cả hai phía Initiator và Responder cùng chạy thuật toán Diffie-Hellman để tìm ra cặp Public key **A** và **B**.

Chi tiết thuật toán được đề cập ở *DH Algorithm – Thuật toán Diffie Hellman (Phần A – I – mục 2.4.5 trong cùng Chapter).*

❖ Step 2-2 : Diffie-Hellman Exchange

Ở *gói tin thứ ba* và *gói tin thứ tư*, Initiator và Responder sẽ trao đổi cặp Public key **A** và **B** cùng với chuỗi Nonce **Ni** và **Nr** cho nhau.

- Initiator gửi Public Key **A** và **Ni** cho Responder.
- Responder gửi Public Key **B** và **Nr** cho Initiator.

Tiếp theo thuật toán Diffie-Hellman sẽ kết thúc bằng việc tạo ra Share Secret Key **K**.

Từ Share Secret Key **K**, Shared Key ID (**SKEYID**) tiếp tục được tạo ra bằng hàm Hash *hashfunc(key, data).*

Phụ thuộc vào cách chọn kiểu xác thực như thế nào mà **SKEYID** sẽ được tạo ra bằng công thức khác nhau. Quá trình **tạo SKEYID** sẽ được nêu cụ thể ở phần tiếp theo.

Từ **SKEYID**, tạo tiếp bộ 3 key

- **SKEYID_A** dùng để xác thực.
- **SKEYID_E** dùng để mã hóa.
- **SKEYID_D** dùng cho non-ISAKMP SA.

SKEYID_D = hashfunc(**SKEYID**, **K**|**Ci**|**Cr**|**0**)
SKEYID_A = hashfunc(**SKEYID**, **SKEYID_D**|**K**|**Ci**|**Cr**|**1**)
SKEYID_E = hashfunc(**SKEYID**, **SKEYID_A**|**K**|**Ci**|**Cr**|**2**)

Do Share Secret Key **K** của Initiator và Responder là giống nhau, cho nên các key **SKEYID, SKEYID_A, SKEYID_E, SKEYID_D** được tạo ra là giống nhau ở cả hai phía Initiator và Responder.

❖ Step 2-3 : Verify the peer Identify

Gói tin thứ năm và *gói tin thứ sáu* sẽ được mã hóa với **SKEYID_E** và xác thực với chuỗi Hash **HASHi** và **HASHr.**

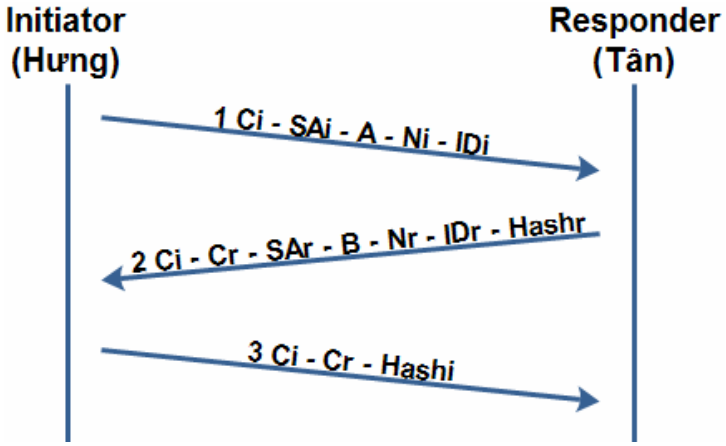
HASHi = hashfunc(**SKEYID, A**|**B**|**Ci**|**Cr**|**SAr**|**IDi**)
HASHr = hashfunc(**SKEYID, A**|**B**|**Cr**|**Ci**|**SAi**|**IDr**)

Trong *gói tin thứ năm* và *gói tin thứ sáu* sẽ kèm theo giá trị xác định danh tính – identification của Initiator và Responder **IDi** và **IDr**.

Một điều cần chú ý là trong Main Mode, bởi vì giá trị **IDi** ở *gói tin thứ năm* đã được encrypted, cho nên phía Responder sẽ hoàn toàn không biết là đang giao tiếp với ai. Cho nên trong trường hợp sử dụng Pre-shared Key cách nhận biết duy nhất là thông qua Source IP của phía Initiator.

2.5.2.2 Aggressive Mode

Aggressive Mode chỉ sử dụng 3 gói tin để đàm phán thay vì 6 như ở Main Mode. Như vậy tốc độ làm việc ở Phase I sẽ được tăng lên đáng kể. Tuy nhiên, cái giá để có được tốc độ đó là khả năng bảo mật bị giảm.



Hình A2 – 10 : Aggressive Mode

Ở *gói tin thứ nhất*, Initiator gửi bộ Policy SAi, chuỗi cookie **Ci**, DH Public key **A**, giá trị Nonce **Di** và giá trị xác định danh tính **IDi** cho Responder.

Ở *gói tin thứ hai*, Response gửi trả lời chuỗi **Cr**, DH Public key **B**, giá trị Nonce N**r** và giá trị xác định danh tính **IDr**, giá trị xác thực **HASHr**.

Ở *gói tin thứ ba*, Initiator gửi giá trị xác thực HASHi cho Response.

Aggressive Mode thường được dùng trong Remote Access VPN, vì khi sử dụng Remote Access thì Responder (tức VPN Gateway) không hề biết gì về địa chỉ của Initiator (Remote Users) và Pre-shared Key được chọn như là phương pháp xác thực.

Aggressive Mode kém bảo mật hơn Main Mode vì các thông tin định danh được gửi ở dạng cleartext và các tham số của DH không được đàm phán.

2.5.2.3 Authentication Method

❖ Prehared Key

Pre-shared Key sẽ được thiết lập trước bằng Out-of-Band. Cho nên cả hai phía Initiator và Responder phải có cùng Pre-shared Key mới thiết lập được IKE Phase I.

Từ Pre-shared Key, giá trị **SKEYID** sẽ được tạo ra bằng hàm Hash

SKEYID = hashfunc(PreShared Key, **Ni|Nr**)

Nhược điểm của Pre-shared Key là trong Main Mode, Pre-shared Key đã được encrypted, nếu Pre-shared Key bị lộ hoặc bị Hacker tấn công bằng BruteForce thì sẽ lộ ra điểm yếu. Cho nên Pre-shared Key được khuyến cáo chỉ sử dụng trong môi trường Remote Access, môi trường mà địa chỉ của Initiator không xác định và chỉ có cách xác thực duy nhất là dùng Pre-shared Key hoặc Certificate cấp cho User.

Hạn chế khác là Pre-shared Key không có tính mở rộng, vì mỗi cặp VPN Gateway phải tạo một bộ Pre-shared Key khác nhau.

❖ Digital Signature

Khi sử dụng Digital Signature, thì các Peer có thể xác thực thông qua Public Key Signature của DSS hoặc RSA.

Public Key thường được đảm bảo thông qua Certificate. Do đó IKE cho phép trao đổi Certificate để xác thực lẫn nhau.

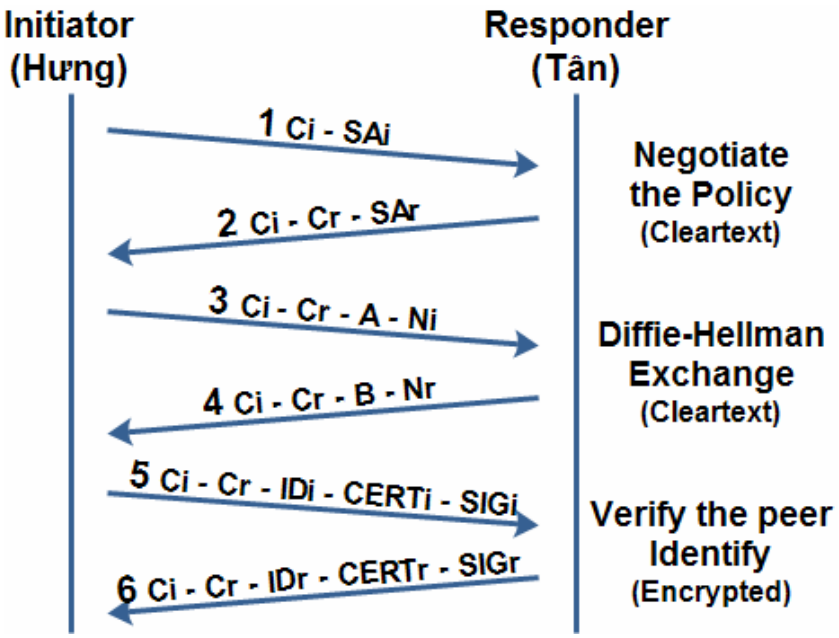
Với Digital Signature thì ở *gói tin thứ ba* và *gói tin thứ tư* sẽ có yêu cầu gửi Certificate. Và ở *gói tin thứ năm* và *gói tin thứ sáu*, Certificate sẽ được trao đổi.

Sự khác biệt giữa xác thực bằng Pre-shared Key và Digital Signature là ở *gói tin thứ năm* và *gói tin thứ sáu*, Pre-shared Key dùng chuỗi **HASHi** và **HASHr** để xác thực, còn đối với Digital Signature thì sẽ thêm một bước là dùng chuỗi **HASHi** và **HASHr** được ký bằng Private Key để xác thực.

HASHi = hashfunc(**SKEYID, A|B|Ci|Cr|SAr|IDi**)

HASHr = hashfunc(**SKEYID, A|B|Cr|Ci|SAi|IDr**)

SIGi = PRIVATEKEY_i(**HASHi**)
SIGr = PRIVATEKEY_r(**HASHr**)



Hình A2 – 11 : Main Mode with Certificate

Chuỗi SKEYID sẽ được tính bằng hàm Hash

SKEYID = hashfunc**(Ni|Nr|K)**

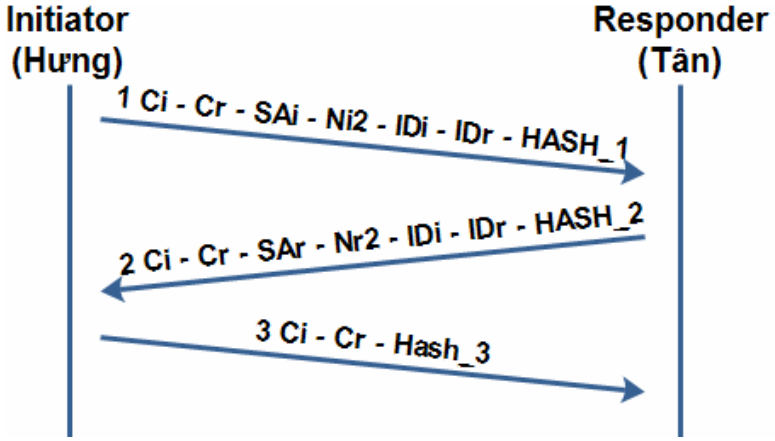
Cả hai phía sau khi nhận được chuỗi **SIGi** và **SIGr** sẽ dùng Public key trong Certificate để decrypted.

2.5.3 Step 3 : IKE Phase II

Mục đích của Phase II là đàm phán bộ IPsec Policy (Phase II Policy), thiết lập đường kết nối an toàn giữa VPN Gateway peers cho việc truyền dữ liệu bằng hay giao thức là ESP và AH.

IKE Phase II hoạt động ở Quick Mode và sử dụng 3 gói tin để đàm phán.

Quá trình đàm phán của IKE Phase II được bảo vệ bởi IKE SA, cho nên các gói tin của IKE Phase II sẽ được encrypted bằng SKEYID_E và xác thực bằng SKEYID_A.



Hình A2 – 12 : Quick Mode

❖ Gói tin thứ nhất

Gói tin thứ nhất đi từ phía Initiator chứa bộ Policy **SAi** cho IKE Phase II, chuỗi Nonce được tạo mới **Ni2** và chuỗi **HASH_1** để xác thực.

Mục đích việc tạo chuỗi Nonce mới là để tạo mới bộ key, bên cạnh đó còn chống được Replay-Attack.

Để chống lại việc Hacker có thể can thiệp vào quá trình hoạt động của IKE Phase II, thì chức năng Perfect Forward Secrecy (PFS) được sử dụng để tạo bộ key cho IKE Phase II.

Khi PFS được kích hoạt thì thuật toán DH sẽ tạo lại bộ Public Key **X**, **Y** mới thay cho bộ **A**, **B** cũ ở Phase I, do đó Share Secret Key **K2** cũng sẽ khác **K**.

Khi đó chuỗi **HASH_1** sẽ có hai trường hợp

HASH_1 = hashfunc(**SKEYID_A**, **Mid**|**SAi**|**Ni2**) khi không có PFS

HASH_1 = hashfunc(**SKEYID_A, Mid**|**SAi**|**Ni2**|**X**|**IDi**|**IDr**) với PFS

Với Mid là Message ID là giá trị dùng để nhận biết một phiên tạo IPSec. Vì cùng một lúc VPN Gateway có thể tham gia vào nhiều VPN Community khác nhau, nêu Mid là một giá trị để phân biệt các phiên tạo kết nối. Giá trị Mid sẽ không bị encrypted.

❖ Gói tin thứ hai

Ở gói tin thứ hai thì Responder sẽ gửi trả về bộ Policy **SAr** phù hợp, chuỗi Nonce được tạo mới **Nr2** cùng chuỗi **HASH_2.**

HASH_2 = hashfunc(**SKEYID_A', Mid**|**SAr**|**Ni2**|**Nr2**) khi không có PFS
HASH_2 = hashfunc(**SKEYID_A', Mid**|**SAr**|**Ni2**|**Nr2**|**Y**|**IDi**|**IDr**) với PFS

❖ Gói tin thứ ba

Gói tin thứ ba thì phía Initiator sẽ xác thực với chuỗi **HASH_3**. Giá trị này dùng để xác thực Initiator vì khi này Initiator đã có cả hai chuỗi **Ni2** và **Nr2.** Nếu **HASH_3** không phù hợp, tức Attacker đã dùng các gói tin Quick Mode của phiên giao dịch trước để tấn công Replay-Attack.

HASH_3 = hashfunc(**SKEYID_A',0|Mid|Ni2|Nr2**)

Kết quả đàm phán của IKE Phase II là bộ IPsec SAs.

2.5.4 Step 4 : Data Transfer

Sau khi IKE Phase II hoàn thành, thì quá trình truyền dữ liệu của người dùng được bắt đầu. Tất cả dữ liệu thỏa yêu cầu của Access Control Policy sẽ được bảo vệ bằng đường IPsec VPN.

2.5.5 Step 5 : IPsec Tunnel Termination

Một kết nối IPsec sẽ kết thúc khi thời gian tồn tại – Life time của IPsec SA kết thúc (Sau một khoảng thời gian hoặc đạt tới mức dung lượng xác định).

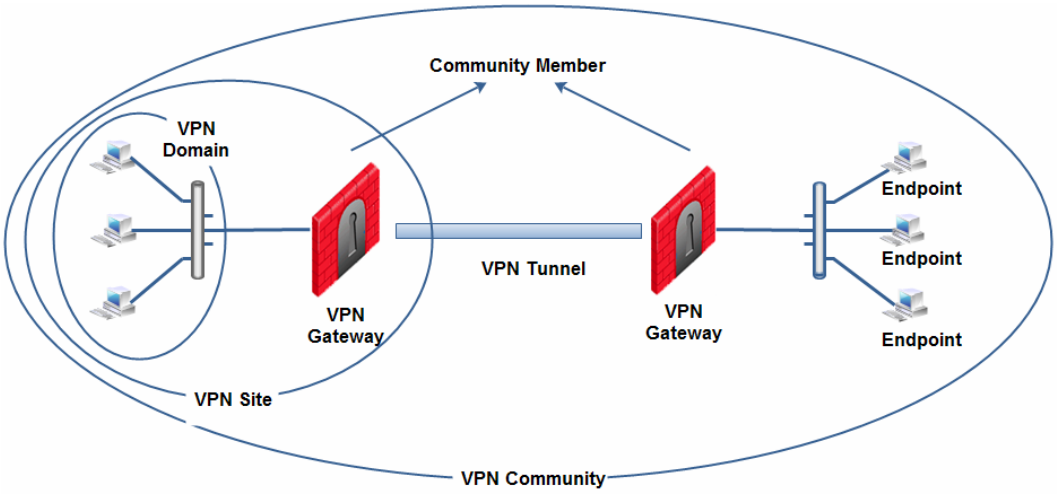
Sau khi kết nối IPsec kết thúc thì IKE Phase II sẽ đàm phán lại tạo kết nối IPsec mới, hoặc cả IKE Phase I sẽ đàm phán lại nếu IKE SA hết thời gian tồn tại.

Sau khi đàm phán lại thì đường IPsec mới sẽ dùng bộ IPsec SA mới.

Thông thường các bộ SA mới sẽ được dàm phán trước khi bộ SA cũ hết thời gian tồn tại, cho nên hoạt động của IPsec luôn liên tục mà không hề có sự gián đoạn.

2.6 VPN Communities and Terminology

- VPN Gateway (VPN Community member)
  - Nói đến các Gateway tham gia vào việc tạo kết nối VPN.
  - VPN Gateway đảm nhận việc encrypted/decrypted dữ liệu.
  - VPN Gateway có thể là một phần mềm tích hợp, một module chuyên dụng hoặc có thể là cả một cluster (Tăng khả năng Availability và LoadSharing).
- VPN Domain (Encryption Domain)
  - Là các host, các network nằm phía sau Gateway, dữ liệu giữa các VPN domain sẽ được encrypted.
  - VPN domain sẽ quy định các host, network nào sẽ sử dụng đường VPN, nên những network không cần thiết như DMZ đều không thuộc VPN domain.
- Endpoint
  - Là các người dùng, thiết bị cụ thể trong VPN Domain.
- VPN Site
  - Là tập hợp Gateway và các VPN domain sau Gateway đó.
  - Một VPN Site thường là một chi nhánh của công ty, các tổ chức ngang hàng…
- VPN Community
  - Là đường kết nối VPN cùng với những thuộc tính của đường VPN đó (thuật toán mã hóa, thuật toán Hash, DH…).



Hình A2 – 13 : VPN Terminology

2.7 IKE DoS Attack and Protection

2.7.1 IKE DoS Attack

Denial of Service – DoS Attack là phương pháp tấn công nhằm vào khả năng xử lý của hệ thống máy tính, làm hệ thống quá tải, khiến người dùng thật sự không thể truy cập được vào dịch vụ hoặc làm tê liệt cả dịch vụ đó.

DoS không phải là mối đe dọa trực tiếp tới tính bí mật dữ liệu của người dùng hoặc chiếm quyền hệ thống. DoS chỉ đơn giản sử dụng hết tài nguyên của hệ thống (Như CPU, RAM…) để hệ thống không thể xử lý được những yêu cầu từ phía người dùng.

Có hai dạng tấn công DoS

- Dạng thứ nhất : Gửi các gói tin rác để làm service bị lỗi và crash.
- Dạng thứ hai : Khai thác các lỗ hổng của service hay protocol bằng cách gửi các gói tin có khuôn mẫu (Well-form packet). IKE DoS Attack thuộc dạng tấn công này.

IKE DoS Attack sẽ tạo ra các gói tin đầu tiên ở IKE Phase 1 với Source IP khác nhau, khiến Gateway phải xử lý các gói tin đó liên tục.

Quá trình xử lý liên tục của Gateway sẽ tiêu tốn một lượng lớn tài nguyên của Gateway về CPU và RAM, khiến Gateway trở nên quá tải và những yêu cầu từ phía người dùng hợp pháp sẽ không được đáp ứng.

2.7.2 Checkpoint Solution

Khi số lượng các kết nối đàm phán IKE vào Gateway tăng lên vượt mức ngưỡng, thì Gateway sẽ quá tải hoặc đang bị IKE DoS Attack. Trong trường hợp này Gateway sẽ lọc ra các peer có độ tin tưởng và các peer có sự nghi ngờ là nguồn của DoS Attack.

Có hai dạng bảo vệ Gateway trước các cuộc IKE DoS Attack

- Stateless Protection.

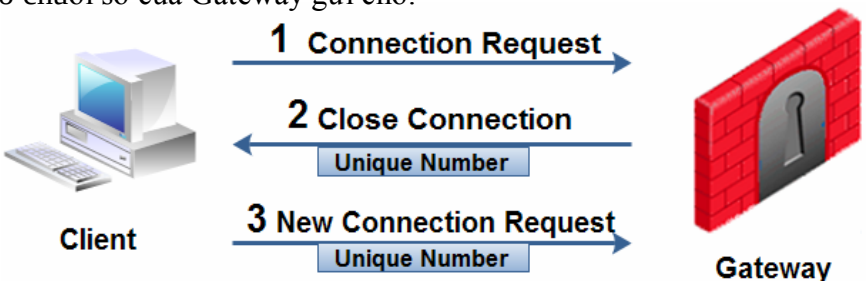
- Puzzles Protection.

2.7.2.1 Stateless Protection

Stateless Protection sẽ hoãn lại việc cấp tài nguyên cho một peer để tạo kết nối cho tới khi peer đó chứng minh được nó là người dùng hợp pháp.

Nếu Gateway đang trong tình trạng quá tải hoặc bị IKE DoS Attack, khi nhận được một yêu cầu kết nối IKE, Gateway sẽ trả lời lại bằng một gói tin chứa một chuỗi số do Gateway tạo ra. Khi đó Gateway sẽ không xử lý yêu cầu tạo kết nối IKE mà chỉ lưu lại trạng thái của chuỗi số Gateway gửi đi.

Phía tạo kết nối khi nhận được gói tin từ Gateway sẽ phải tạo lại kết nối IKE khác kèm theo chuỗi số của Gateway gửi cho.



Hình A2 – 14 : Stateless Protection

Phía Gateway khi nhận được kết nối IKE chứa chuỗi số đó sẽ đồng ý thiết lập kết nối dù cho Gateway đang trong tình trạng quá tải.

Nếu Gateway nhận được nhiều kết nối IKE từ nhiều IP khác nhau thì mỗi IP sẽ được trả lời với các chuỗi số khác nhau, và mỗi IP đều được yêu cầu tạo kết nối IKE mới với chuỗi số mà nó nhận được. Do đó nếu IP đó là IP giả mạo (IP Spoofing) thì Gateway sẽ không bao giờ nhận được chuỗi số đó từ attacker. Từ đó sẽ khiến cho attacker thất bại trong việc gửi hàng loạt kết nối IKE từ nhiều IP khác nhau.

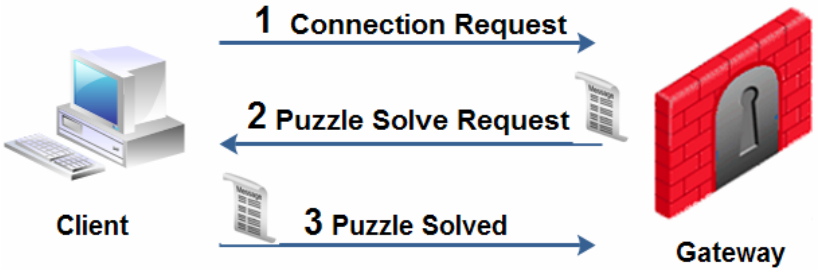
2.7.2.2 Puzzles Protection

Điểm yếu của Stateless Protection đó là chỉ có khả năng bảo vệ Gateway trước các kết nối từ một nguồn xác định (như một peer Gateway với địa chỉ tĩnh) hoặc những attacker có kiến thức kém về VPN.

Trong trường hợp Attacker sử dụng nhiều địa chỉ IP khác nhau để tạo kết nối IKE với chuỗi số tạo kết nối bất kỳ, thì đến một lúc nào đó Gateway cũng sẽ bị hạ gục.

Như vậy trong trường hợp các nguồn kết nối không xác định được source (như từ một peer Gateway với DAIP hoặc SecuRemote/SecureClient) thì phương pháp Puzzles Protection là lựa chọn tốt nhất.

Thay vì sử dụng chuỗi số để ngăn ngừa IKE DoS Attack thì Puzzles Protection sẽ yêu cầu phía tạo kết nối phải giải một bài toán phức tạp. Để giải được bài toán đó thì mỗi máy phải tốn một khoảng thời gian ngắn (vài bài toán trong một giây). Tuy nhiên, với khoảng thời gian đó cũng đủ khiến cho việc tấn công DoS thất bại (vì chỉ vài yêu cầu tạo kết nối được gửi trong một giây).



Hình A2 – 15 : Puzzles Protection

2.8 Access Control and VPN Communities

Cấu hình các VPN Gateways vào một VPN Community nghĩa là nếu các VPN Gateway đó được phép giao tiếp với nhau thông qua các Access Control Policy thì traffic của giao tiếp đó sẽ được encrypted.

Cấu hình Access Control Policy là ở thẻ Firewall trên SmartDashboard. Thông qua cột "VPN" có trong Access Control Policy, ta có thể quy định những kết nối nào là thuộc một VPN Community xác định.

Như vậy việc đặt các Access Control Policy để quản lý các kết nối có hay không được sử dụng đường VPN là hết sức quan trọng. Bởi vì không phải kết nối nào cũng từ Site này sang Site khác, mà có những kết nối từ host trong mạng Private truy cập ra Internet hoặc vào một vùng khác như DMZ.

Ví dụ ta có cặp Access Control Policy như sau

Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1		LAN_NVT LAN_QT	LAN_QT LAN_NVT	HoaSen_Commu	TCP http	accept	Log	QT	Any
2		LAN_QT	Any	Any Traffic	TCP http	accept	None	QT	Any

Hình A2 – 16 : Access Control Rule Example

- Nếu các kết giữa hai vùng Private Quang Trung và Nguyễn Văn Tráng sử dụng dịch vụ HTTP thì các kết nối đó sẽ được mã hóa và đi đường VPN.
- Nếu kết nối từ vùng Private Quang Trung ra mọi nơi (trừ vùng Private Nguyễn Văn Tráng) và sử dụng dịch vụ HTTP sẽ không được encrypted.

Trong trường hợp kết nối từ vùng Private không được encrypted đi ra vùng Public thì ta cần phải đặt thêm NAT Rule, đồng thời ta phải Disable chức năng NAT trong đường VPN để cả hai Access Control Policy hoạt động bình thường và hiệu quả.

C . Remote Access VPN

1 Overview

1.1 Need for Remote Access VPN

Trong một số trường hợp, người dùng ở xa có nhu cầu kết nối tới công ty để làm việc, up/down dữ liệu, thì điều quan trọng ở đây phải đảm bảo những đường kết nối đó sẽ an toàn, nhanh chóng và đạt hiệu quả cao.

Thừa hưởng những đặc tính của IPsec VPN (Bảo mật, đảm bảo toàn vẹn dữ liệu và có cơ chế xác thực chính xác), Remote Access VPN đem lại cho người dùng từ xa – Remote Users những ưu điểm như sau

- Đảm bảo tính an toàn về dữ liệu.
- Tạo kết nối an toàn từ người dùng về công ty.
- Cơ chế xác thực hiệu quả.
- Hạn chế tối đa những bước cấu hình phức tạp.
- Sử dụng mọi lúc mọi nơi (Chỉ cần có kết nối Internet).
- Không yêu cầu thiết bị đặc biệt để thiết lập kết nối.
- Áp đặt các chính sách lên người dùng ở xa.

Remote Access VPN được sử dụng trong nhiều trường hợp như

- Người dùng thường xuyên thay đổi vị trí.
- Vị trí khởi kết nối của người dùng thường xuyên thay đổi (Sáng kết nối tới Headquarters, chiều kết nối tới Branch).
- Người dùng sử dụng môi trường kết nối là Wireless.

1.2 Checkpoint Solution

Checkpoint có ba giải pháp Remote Access VPN dành cho doanh nghiệp

- Sử dụng Secureclient (SecureClient/SecuRemote – Endpoint Connect – Endpoint Security – SecureClient Mobile).
- SSL.
- SSL Network Extender.

Các sản phẩm cung cấp Remote Access VPN chính của Checkpoint là Checkpoint Security Gateway và Connectra.

1.2.1 Remote Access and Components

Mô hình Remote Access bao gồm các thành phần sau

- Remote Access Community.
- SecureClient/SecuRemote.

- Connection Mode.
- Users Profiles.
- Access Control.
- Client-Gateway Authentication Schemes.
- Advanced Features.

1.2.1.1 SecureClient/SecuRemote and Features

SecuRemote là phần mềm kết nối Remote Access cho phép người dùng sử dụng Remote Access một cách nhanh chóng và dễ dàng.

SecureClient là phiên bản mở rộng của SecuRemote, thêm vào những chức năng cao cấp, được chia làm ba nhóm chính

- Security features
  - Desktop Security Policy
  - Logging and Alerts
  - Secure Configuration Verification (SCV)
- Connectivity features
  - Hub Mode
  - Office Mode
  - Visitor Mode
- Management features
  - Automatic Software Distribution
  - Avanced Packaging and Distribution Options
  - Diagnostic tools

1.2.1.2 Connection Mode

Phụ thuộc vào mục đích sử dụng và độ bảo mật của hệ thống, các vấn đề của hệ thống mạng thì các Remote Access được chia làm ba dạng kết nối chính

- Hub Mode.
- Office Mode.
- Visitor Mode.

1.2.1.3 User profiles

Là các profile được định nghĩa (Do người dùng định nghĩa hoặc định nghĩa trước bởi người quản trị) để sử dụng đường Remote Access VPN.

User Profiles được sử dụng bởi người dùng, cho phép lưu lại các cấu hình kết nối (Remote Gateway, Policies, Authentication Method…).

User Profiles được sử dụng nhiều cho người dùng mobile (Laptop, smartphone, iPhone/iPad), là dạng Remote Users thay đổi vị trí liên tục, đi kèm theo những rắc rối với hệ thống mạng nơi người dùng (NAT, Firewall).

1.2.1.4 Access Control

Access Control kết hợp với Remote Access Community sẽ tạo ra các quy định sử dụng đường Remote Access và tài nguyên hệ thống như thế nào.

Remote Access Community qui định Users nào được phép dùng Remote Access.

Access Control sẽ quy định Users nào (Sau khi được cho phép dùng Remote Access) được phép dùng tài nguyên và dịch vụ nào, Users nào bị hạn chế quyền sử dụng.

1.2.1.5 Client-Gateway Authentication Schemes

Xác thực là một trong những nhân tố chính tạo nên tính an toàn cho đường kết nối. Hai dạng xác thực được sử dụng chính là Digital certificates và Pre-shared Key.

Ngoài ra còn các dạng xác thực khác như One Time Password, SecurID…

- Digital certificates.

  Digital Certificate là phương pháp xác thực đơn giản và hiệu quả nhất trong Remote Access VPN. Cả hai phía Remote User và Remote Access Gateway đều phải có Certificate để xác thực lẫn nhau.

  Certificate sử dụng phải được xác định là có hiệu lực

  - Được cấp bởi Trusted CA.
  - Vẫn còn giá trị sử dụng (Chưa hết hạn hoặc bị thu hồi - Revoked).

  Certificate có thể được cấp bởi hai nguồn

  - Internal CA (Do chính Remote Access Gateway cấp).
  - External CA (Third Party CA).

  Certificate được tạo và gửi đến người nhận qua Out-of-band.

- Pre-shared Key

  Cả hai phía Remote User và Remote Access Gateway sẽ được tạo bộ key giống nhau. Khi xác thực thì Remote User gửi Pre-shared Key cho Remote Access Gateway, nếu đúng chính xác key thì kết nối được tạo.

  Mỗi Remote User sẽ có một Pre-shared Key khác nhau.

  Xác thực bằng Pre-shared Key sẽ không an toàn bằng Certificate, vì các Pre-shared Key có thể giống nhau còn Certificate là độc nhất.

1.2.1.6 Advanced Features

Một số chức năng mở rộng của Remote Access là sử dụng L2TP để kết nối hoặc cấp IP per User/Group.

1.2.2 Connectra and Deloyment

Connectra là một thiết bị chuyên dụng (Connectra Appliance) hoặc có thể là một máy tính cài phần mềm Connectra (Connectra Software) được dùng như một cổng kết nối – Remote Access Gateway với nhiều chức năng tiên tiến như

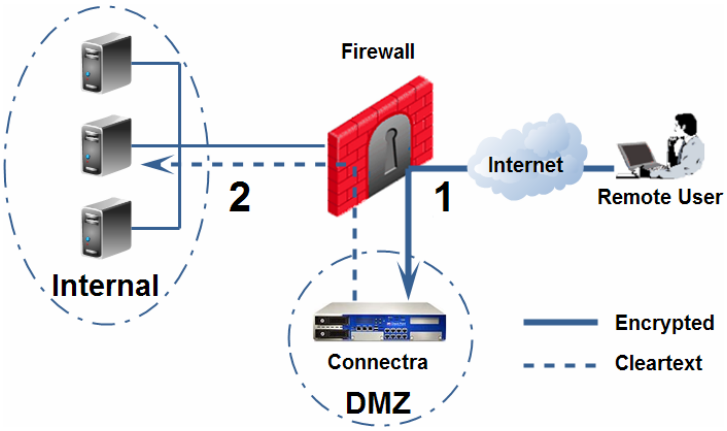
- Hỗ trợ kết nối an toàn qua nền Web – SSL.
- Tích hợp sẵn IPS.
- Dễ dàng quản lý.
- Hỗ trợ Endpoint Connect Client.
- Thích ứng và hỗ trợ Endpoint Security.
- Hỗ trợ xác thực SecurID và SMS.

Hai mô hình triển khai Connectra vào hệ thống thường được sử dụng là triển khai Connectra vào vùng DMZ và triển khai Connectra vào LAN. Nhưng thông thường Connectra được triển khai chủ yếu vào vùng DMZ.

Dù là ở dạng triển khai nào thì kết nối từ LAN tới Connectra là trực tiếp, còn từ Internet tới Connectra là thông qua NAT.

1.2.2.1 Deploy Connectra in DMZ

Khi Connectra được triển khai trong DMZ sẽ loại bỏ hoàn toàn các kết nối từ Internet vào LAN.



Hình A3 – 1 : Connectra in DMZ

Các kết nối được tạo từ Users (Từ LAN hoặc từ Internet) sẽ tới thiết bị Firewall. Phụ thuộc vào Access Control Rule ở Firewall mà kết nối sẽ được tiếp tục hay kết thúc.

Nếu kết nối được cho phép thì kết nối được đưa tới Connectra, Connectra sẽ xác thực Remote User. Kết nối từ User tới Connectra được encrypted bằng SSL.

Phụ thuộc vào Access Control Rule trên Connectra (Trong Connectra gọi là Access to Application) mà Remote Users được phép truy cập tài nguyên và dịch vụ trong vùng Internal (Bao gồm LAN, DMZ và Management).

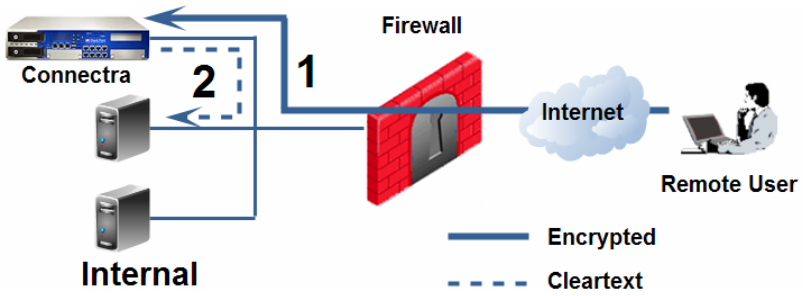
Connectra thay mặt User truy cập tài nguyên, dịch vụ ở vùng Internal, kết nối từ Connectra tới vùng Internal là cleartext (Hoặc là encrypted nếu có nhu cầu).

Như vậy, một ứng dụng trong vùng Internal được cấp quyền sử dụng bởi Connectra lẫn Firewall nếu host chứa ứng dụng không nằm trong vùng DMZ.

1.2.2.2 Deploying Connectra on a LAN

Với Connectra được triển khai trong LAN, thì kết nối từ vùng Internet sẽ trực tiếp đi tới vùng LAN (cụ thể là thiết bị connectra), kết nối này được encrypted bằng SSL.

Nếu có bất kỳ hành vi truy cập bất hợp pháp vào tài nguyên vùng LAN mà không được nhận biết bởi Connectra, thì Firewall không thể ngăn chặn được hành vi đó.



Hình A3 – 2 : Connectra on LAN

1.2.2.3 Deploying a Connectra Cluster

Sự bùng nổ công nghệ hiện tại giúp người dùng càng có nhiều phương pháp học tập hơn. Và hiện tại eLearning là phương pháp học ngoài giờ tốt nhất mà các trường Đại học có thể cung cấp cho sinh viên.

eLearning có thể chứa các bài viết, các bài presentation, các đoạn ghi âm của giảng viên, hoặc có thể là video clip.

Với lượng tài nguyên nhiều cùng số lượng sinh viên sử dụng hệ thống eLearning nhiều sẽ nảy sinh ra vấn đề quá tải cho các cổng kết nối. Từ đó cần có giải pháp cân bằng tải cho các cổng kết nối này, và giải pháp của Checkpoint Connectra Cluster.

1.2.3 User Database

Remote Access Gateway cung cấp nhiều dạng cơ sở dữ liệu – user database để lưu trữ tài khoản của Users (Bao gồm Username, Passwor, Certificate, eMail…).

Các dạng database được hỗ trợ

- Internal
- LDAP
- RADIUS
- SecurID

1.2.3.1 Internal

Cho phép Remote Access Gateway lưu trữ password của Users trên database nội bộ (trên chính Remote Access Gateway). Ứng với mỗi User là một password.

1.2.3.2 LDAP

LDAP là một chuẩn mở được dùng cho nhiều hãng thiết bị khác nhau. Thông qua LDAP thì Users được quản lý trên LDAP server lẫn Remote Access Gateway. Tuy nhiên toàn bộ user database nằm trên LDAP server.

Khi có yêu cầu kết nối của Users đi đến, thì yêu cầu xác thực của Users sẽ được gửi đến LDAP server.

Ngoài việc sử dụng cho Remote Access Gateway, cùng một LDAP user database có thể dùng cho các ứng dụng và thiết bị khác với nhiều mục đích xác thực khác nhau.

1.2.3.3 RADIUS

RADIUS là dạng xác thực thông qua một server bên ngoài, tuy nhiên trên Remote Access Gateway không có quyền quản lý Users như LDAP.

RADIUS cho phép người quản trị tách biệt chức năng xác thực ra khỏi chức năng ủy quyền truy cập.

Cũng như LDAP server, yêu cầu xác thực sẽ được gửi đến RADIUS server.

1.2.3.4 SecurID

SecurID – được phát triển bởi RSA Security – cho phép xác thực bằng hai nhân tố khác nhau (Two-Factor Authentication).

SecurID đòi hỏi người dùng phải có cả thiết bị xác thực Token lẫn số PIN hoặc Password.

Token sẽ tạo one-time Password và đồng bộ với RSA ACE/server. Token có thể là hardware (Smartcard, USB device) hoặc software (RSA Security SID 820).

Hình A3 – 3 : RSA SecurID 800

Hình A3 – 4 : RSA SecurID 900

One-time Password được tạo ra một cách ngẫu nhiên và thay đổi liên tục sau một khoảng thời gian xác định (mặc định là 60 giây).

Khi Users có nhu cầu xác thực thì ở Token lẫn ACE/Serrver đều tạo ra cùng một One-time Password, người dùng phải cung cấp đúng One-time Password so với ACE/Server mới có thể xác thực thành công.

2 Resolving Connectivity Issues

Quá trình triển khai VPN vào thực tế có thể phát sinh rất nhiều trở ngại, vì người dùng Remote Access VPN đa phần nằm ngoài phạm vi quản lý của hệ thống mạng công ty. Họ có thể ở nhà, khách sạn, nhà hàng, nơi công cộng…Những nơi đó luôn có những chính sách mạng riêng như NAT, Firewall…từ đó phát sinh ra các trợ ngại như

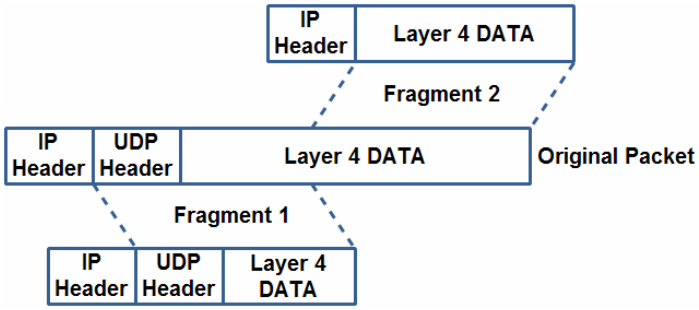
- ❖ NAT không hỗ trợ gói tin bị phân mảnh – Fragmentation Packet.
- ❖ Firewall hạn chế số lượng dịch vụ được phép truy cập.

2.1 NAT Related Issues

2.1.1 Packet Fragmentation

Những phát sinh liên quan tới NAT đa phần do NAT không hỗ trợ việc dựng lại các packet bị phân mảnh.

Khi Remote Users tạo kết nối tới Remote Access Gateway thì những gói tin IKE hoặc IPsec sẽ rất lớn (vượt qua giá trị MTU). Khi thiết bị xác định packet vượt giá trị MTU thì packet sẽ bị phân ra làm nhiều phần, mỗi phần tạo một packet mới (Xảy ra nhiều với các gói tin UDP).



Hình A3 – 5 : Packet Fragmentation

- Packet đầu tiên sẽ chứa UDP header và một phần Layer 4 Data.
- Các packets tiếp theo chỉ chứa Layer 4 Data.

Quy tắc của NAT là thay đổi thông tin của IP header (IP address) lẫn của UDP header (Port number). Khi fragment packet đầu tiên tới thiết bị NAT, thì gói tin đó sẽ được translate thành công. Tuy nhiên các fragment packets tiếp theo sẽ không được thiết bị NAT hiểu do không chứa UDP header, thiết bị NAT khi đó sẽ drop các fragment packet đó đi, đồng nghĩa với việc kết nối Remote Access thất bại.

Ở mỗi gian đoạn của quá trình thiết lập và truyền dữ liệu của Remote Access, thì sẽ có một giải pháp riêng để khắc phục những phát sinh của NAT.

2.1.2 IKE Phase I Problem and Solutions

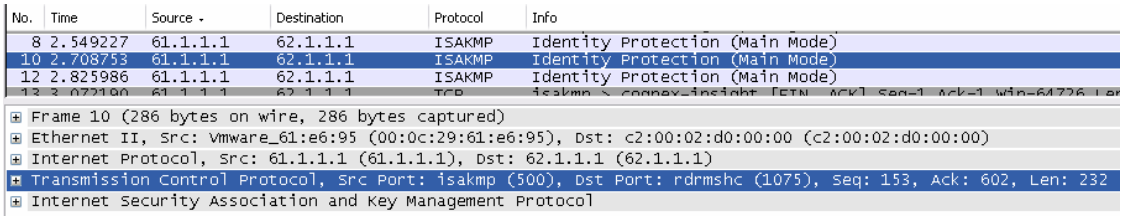
Ở IKE Phase I, thì sẽ có phần xác thực qua lại giữa Remote User và Remote Access Gateway. Có hai phương pháp xác thực chính là Pre-shared Key và Digital Certificate.

Khi sử dụng Certificate thì sẽ có quá trình trao đổi Certificate hoặc cập nhật CRLs (Certificate Revocation Lists). Nếu Certificate hoặc CRLs quá lớn sẽ dẫn tới gói tin IKE Phase I cũng lớn theo. Vậy nên các gói tin IKE Phase I sẽ bị Fragment.

Giải pháp đơn giản nhất ở đây là sử dụng Pre-shared Key. Pre-shared Key đơn giản về mặt cấu hình lẫn hạn chế vấn đề Fragment. Tuy nhiên Pre-shared Key không an toàn và bảo mật như Certificate (Lộ password khi nhập, IKE Pre-shared Key crack…). Vậy trong trường hợp không sử dụng Pre-shared Key thì cần phải có một giải pháp tối ưu hơn.

2.1.2.1 IKE over TCP

Mặc định IKE sẽ sử dụng gói tin UDP để đàm phán kết nối, tuy nhiên trong Remote Access, do vấn đề của NAT mà ta có thể cấu hình cho IKE đàm phán dựa trên gói tin TCP (Gói TCP sẽ không bị Fragment). Ở TCP header, cờ DF (do not fragment) sẽ được bật lên, đồng thời TCP tạo một phiên kết nối đầy đủ (Full TCP session) giữa Remote User và Remote Access Gateway.



Hình A3 – 6 : IKE over TCP Packet

2.1.2.2 IKEv2

Một giải pháp khác là sử dụng IKEv2. Với IKEv2 thì Certificate sẽ được trao đổi thông qua FTP hoặc HTTP. Do đó gói tin IKE Phase I sẽ không vượt quá MTU và bị fragmented.

2.1.3 IKE Phase II Problem and Solutions

Ở Phase II thì quá trình đàm phán bộ Policy dành cho IPsec Tunnel sẽ được thực hiện. Phía Remote Access Gateway sẽ được cấu hình sẵn các bộ Policy xác định. Tuy nhiên ở phía Remote Users lại không được cấu hình sẵn các bộ Policy, mà phần mềm Remote Client sẽ tự tạo ra tất các bộ policy có thể có để phù hợp với Remote Access Gateway, rồi gửi tất cà các bộ policy có được tới Remote Access Gateway. Nếu Remote Access Gateway tìm được bộ policy giống với bộ policy mà Remote Access Gateway đã được cấu hình, kết nối được chấp nhận.

Do đó dẫn tới gói tin ở Phase II rất lớn, vượt qua MTU và bị fragment. Vấn đề fragment lại phát sinh ở IKE Phase II.

Giải pháp IKE over TCP như ở Phase I không thể sử dụng cho Phase II. Bởi vì ở Phase II, quá trình tạo mới key sẽ được thực hiện sau một khoảng thời gian xác định (Hết thời gian sống của SA – SA's Life time hoặc dung lượng IPsec được sử dụng đã hết), và từ phía Remote User lẫn Remote Access Gateway đều có thể khởi tạo kết nối yêu cầu tạo mới key. Giả sử phía Remote Access Gateway khởi tạo kết nối, thì dù Remote Access Gateway biết được địa chỉ IP của thiết bị NAT, cũng không thể khởi tạo kết nối vì Remote Access Gateway không biết port nào trên thiết bị NAT sẽ được gán cho Remote User (do NAT thay đổi port gán cho Users liên tục sau mỗi kết nối), hoặc tệ hơn là thiết bị NAT không hỗ trợ cho phép Remote Access Gateway khởi tạo kết nối vào Remote User.

Giải pháp IKE over TCP trên thực tế có thể sử dụng được, tuy nhiên phải đảm bảo cho kết nối của Remote Access Gateway và Remote Users luôn được mở (Static NAT, dành riêng cho các kết nối này các socket riêng hoặc liên tục gửi gói Keep-alive). Tuy nhiên làm như vậy sẽ tốn tài nguyên của hệ thống NAT và có thể thiết bị NAT đó không hỗ trợ cho người dùng.

❖ Small IKE Phase II Proposals

Giải pháp tốt nhất là phía Remote Access Gateway và Remote User cùng khởi tạo các bộ policy với số lượng nhỏ các thuật toán Encryption và Integrity (Sử dụng các thuật toán thường được sử dụng).

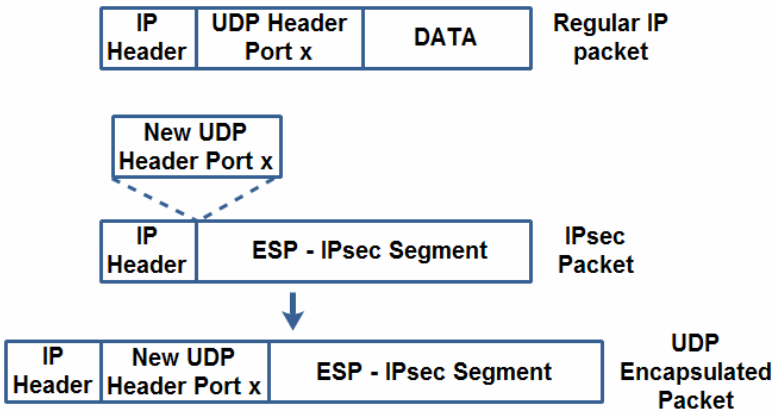
Nếu không có bộ policy nào trong số các bộ policy được gửi bởi Remote User phù hợp với Remote Access Gateway, thì số lượng đầy đủ các bộ policy sẽ được gửi.

Thông thường thì Remote Access Gateway sẽ dễ dàng tìm được bộ policy phù hợp trong số các bộ policy hạn chế được gửi bởi Remote User. Tuy nhiên vẫn có trường hợp không tìm được bộ policy thích hợp (Hay xảy ra nếu Remote Access Gateway sử dụng thuật toán mã hóa AES-128, vì AES-128 không nằm trong số các thuật toán dùng trong Small IKE Phase II Proposals), cho nên ta cần chú ý vấn đề này khi thiết lập hệ thống Remote Access.

2.1.4 IPsec Data transfer Problem and Solutions

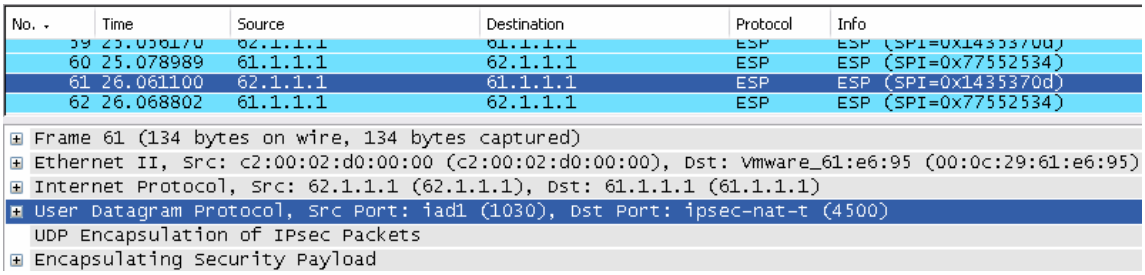
2.1.4.1 NAT Traversal

Trong giai đoạn truyền dữ liệu của IPsec, dữ liệu của người dùng sẽ được mã hóa, toàn bộ thông tin từ Layer 3 trở lên (Bao gồm IP header và Layer 4 Header) sẽ bị mã hóa, một IP header mới được thêm vào. Do đó thiết bị NAT không thể biết được nội dung có trong Layer 4 Header, trong đó chứa thông tin port number của gói tin. Kết quả là thiết bị NAT không thể translate gói tin IPsec, gói tin IPsec sẽ bị drop.



Hình A3 – 7 : NAT Traversal Packet – 1

Giải pháp ở đây là ta sẽ đóng gói – Encapsulate các IPsec Segment bằng UDP, còn IP header vẫn giữ nguyên. Như vậy thì khi gói tin IPsec tới thiết bị NAT thì thiết bị NAT có thể translate gói tin ESP đó như một gói UDP bình thường.



Hình A3 – 8 : NAT Traversal Packet – 2

Port thường sử dụng cho "New UDP Header" là 4500 được qui định ở IANA.

2.1.4.2 IPsec PMTU

Trước khi truyền dữ liệu, thì IPsec sẽ phải tìm xem đâu là giá trị MTU thích hợp để khi truyền trên internet, các gói tin của IPsec không bị fragmented.

PMTU - Path Maximum Transmission Units là giá trị MTU nhỏ nhất trong số các giá trị MTU của các router trên đường đi của gói tin.

Do giá trị MTU của các router là khác nhau, nên cần có cơ chế xác định giá trị PMTU sao cho chính xác. Có hai phương pháp để xác định PMTU

- Active IPSec PMTU
- Passive IPSec PMTU

❖ Active IPSec PMTU

Sau khi kết thúc đàm phán ở Phase II và trước khi dữ liệu được truyền trên đường IPsec, thì Remote User sẽ thực hiện việc gửi nhiều gói tin với độ lớn khác nhau. Các gói tin được gửi đều có cờ DF (Do not Fragment) được bật.

Khi router nào nhận được gói tin

- Nếu gói tin có dung lượng nhỏ hơn MTU của router thì gói tin được phép đi qua.
- Nếu gói tin có dung lượng lớn hơn MTU của router thì gói tin sẽ bị drop, đồng thời router gửi trả về cho Remote User gói ICMP báo lỗi.

Dựa vào gói tin có dung luợng lớn nhất đi tới được đích mà không bị báo lỗi, thì Remote User có thể tìm ra giá trị PMTU.

❖ Passive IPSec PMTU

Với Active PMTU, thì vấn đề sẽ khó khăn hơn nếu đường đi của gói tin được định tuyến động – Dynamic Routing.

Passive IPsec PMTU sẽ giải quyết vấn đề này bằng cách vẫn gửi dữ liệu trên đường IPsec như bình thường, nhưng tất cả các gói tin IPsec đều được bật cờ DF. Như vậy nếu có bất kỳ router nào có giá trị MTU nhỏ hơn dung lượng của gói tin, thì gói tin sẽ bị drop, và một gói ICMP sẽ được gửi trả về cho Remote Access Peers (là Remote Access Gateway hoặc Remote User).

Khi Remote Access Peers nhận được gói ICMP đó, thì Remote Access Peers sẽ truyền lại gói tin bị drop và giảm giá trị PMTU hiện tại xuống.

Trên thực tế thì cả hai cơ chế này hoạt động một cách tự động. Vì cách tìm PMTU là giải thuật được sử dụng chung cho nhiều giao thức.

2.2 Restricted Internet Access Issues

2.2.1 Overview

Remote Userss tạo kết nối tới Remote Access Gateway thông qua hệ thống mạng công cộng (Dịch vụ Internet, khách sạn, nhà hàng, thư viện…), thì người quản trị những hệ

thống mạng công cộng đó có thể hạn chế các dịch vụ mà người dùng có thể truy cập. Thông thường hai dịch vụ thường được cho phép nhiều nhất là HTTP và HTTPS.

Vấn đề nảy sinh ở đây là IPsec chạy ở port 500 (cho quá trình đàm phán ISAKMP), như vậy vô tình người dùng không thể sử dụng Remote Access theo cách thông thường được nữa vì Firewall đã hạn chế dịch vụ.

2.2.2 Checkpoint Solution – Visitor Mode

Visitor Mode cho phép Remote Users có thể tạo kết nối tới Remote Access Gateway thông qua cổng SSL (port 443).

Để chạy được chế độ này thì ở cả hai phía đều phải được hỗ trợ Visitor Mode.

- Ở Remote Access Gateway phải kích hoạt chức năng này.
- Ở Remote Users phải sử dụng SecureClient và kích hoạt chức năng này.

2.2.2.1 Number of Users

Để có được hiệu năng tốt nhất khi sử dụng Visitor Mode

- Hạn chế tối đa số lượng Users sử dụng Visitor Mode, chỉ dùng khi cần thiết.
- Tăng số lượng sockets có thể sử dụng cho Visitor Mode.

2.2.2.2 Allocating Customized Ports

Ngoài sử dụng port SSL 443 ra thì Checkpoint còn hỗ trợ sử dụng các port khác cho Visitor Mode. Khi sử dụng port khác port 443 thì ta cần phải cấu hình ở Access Remote Gateway lẫn có sự cho phép sử dụng ở thiết bị Firewall phía Remote Users.

2.2.2.3 Visitor Mode and Proxy Servers

Visitor Mode còn có thể sử dụng được khi phía Remote Users có sử dụng Proxy server. Trong trường hợp này thì Remote Users sẽ kết nối tới Remote Access Gateway thông qua Proxy server.

2.2.2.4 Visitor Mode and Port 443 is Occupied By HTTPS server

Một phát sinh khi sử dụng Visitor Mode là có thể port 443 sử dụng cho Visitor Mode đang bị sử dụng bởi một ứng dụng khác (SSL Network Extender, Static NAT tới một Server, sử dụng cho Connectra…) trên Remote Access Gateway. Khi đó các kết nối tới Remote Access Gateway sẽ được báo lỗi là

> "Visitor Mode Server failed to bind to xxx.xxx.xxx.xxx:yy (either port was already taken or the IP address does not exist)"

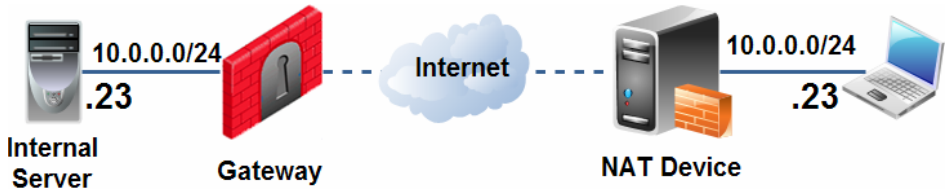
Để giải quyết trường hợp phát sinh này ta có thể sử dụng hai Interface cho phía External (Cả hai đều có IP Pulic), một phục vụ cho Visitor Mode, một phục vụ cho HTTP server.

3 Office Mode

3.1 Overview

Khi Remote Users sử dụng dịch vụ mạng công cộng để tham gia vào Remote Access, thì Remote Users có thể sẽ nằm phía sau một thiết bị NAT và được cấp địa chỉ Private (Non-Routable), chính vì được cấp đỉa chỉ Private cho nên khi Remote Users sử dụng Remote Access sẽ xảy ra nhiều mâu thuẫn.

- ❖ Firewall của công ty chỉ cho phép một số dịch vụ được truy cập bởi Internal Users. Nếu Remote Users không được cấp đúng địa chỉ thì không thể truy cập.
- ❖ Địa chỉ của Remote Users được cấp bởi internet công cộng trùng với địa chỉ mạng vùng Internal của công ty, thậm chí địa chỉ IP của Remote Users được cấp trùng với địa chỉ host chứa tài nguyên mà Remote Users cần truy cập.



Hình A3 – 9 : Office Mode Problem

- ❖ Hai Remote Users được cấp cùng một địa chỉ IP, khi truy cập vào cùng một tài nguyên, thì tài nguyên của công ty sẽ không biết trả lời cho Remote User nào.

3.2 Checkpoint Solution - Office Mode

Giải pháp của Checkpoint là sử dụng Office mode. Với Office mode thì mỗi Remote User sẽ được cấp một IP khi kết nối tới Remote Access Gateway và được xác thực thành công.

Địa chỉ được cấp có thể là từ chuỗi địa chỉ được xác định sẵn – IP Pool, thông qua DHCP server hoặc địa chỉ được cấp riêng cho các group User.

Ngoài địa chỉ IP, Remote Users còn được cấp cho địa chỉ DNS và WINS để có thể phân giải tên miền trong vùng Internal.

Office Mode hỗ trợ các dạng kết nối thông qua

- SecureClient.
- SSL Network Extender.
- L2TP.

3.3 How Office Mode Works

Khi Remote Users khởi tạo kết nối tới Remote Access Gateway, quá trình đàm phán IKE sẽ diễn ra như bình thường, tuy nhiên ở giữa IKE Phase I và IKE Phase II sẽ chạy một mode gọi là Config-mode.

Config-mode sẽ đảm nhiệm việc cấp địa chỉ IP, DNS server, WINS server. . .

Sau khi các địa chỉ IP được Remote Access Gateway cấp sẽ được gán cho một Virtual Interface (cổng ảo) trong hệ điều hành của Remote Users. Những gói tin được định tuyến về mạng Internal sẽ đi qua Virtual Interface này.

Trước khi gói tin đi qua NIC thật thì gói tin sẽ được đóng gói bằng IPsec (hoặc SSL) với Source IP là của NIC thật.

Dãy IP được cấp cho Remote Users phải là dãy địa chỉ có thể định tuyến được từ Remote Access Gateway, bởi vì gói tin response phải được trả về cho Remote Users.

3.4 Workflow

Khi một packet từ Remote Users được gửi đi, nếu Destination IP là thuộc mạng Private của công ty, thì packet đó sẽ đi qua Virtual Interface.

Packet đó sẽ có Source IP là IP của Virtual Interface, Destination là của host trong mạng của Private công ty.

Packet sau khi ra khỏi Virtual Interface sẽ được encrypt với IPsec, đồng thời encapsulate packet với UDP header có thể được NAT và định tuyến.

IPsec Packet sẽ có Source IP là IP của Interface thật (Do ISP hoặc DHCP Server của mạng công cộng cấp), Destination IP là IP của Remote Access Gateway.

Remote Access Gateway sau khi nhận được IPsec Packet sẽ de-encapsulate và decrypted cho ra gói packet gốc, packet gốc này sau đó sẽ được định tuyến đi đến host theo Destination IP.

Khi host trả lời lại packet nhận được, packet tới Remote Access Gateway thì Remote Access Gateway sẽ làm tương tự như Remote User (encrypt và encapsulate) để trả về cho Remote User.

3.5 IP Address Allocation

Có ba phương pháp cấp IP cho Remote Users

- IP Pool
- DHCP Server
- RADIUS Server

3.5.1 IP Pool

Quản trị viên sẽ tạo ra các IP Pool trên Remote Access Gateway, khi Remote Users kết nối vào Remote Access Gateway thì Remote Access Gateway sẽ tự động cấp các địa chỉ IP trong IP Pool đã được tạo.

IP được cấp sẽ là IP độc nhất (tránh trường hợp trùng IP).

IP Pool có thể cấp IP dựa trên source IP (ứng với một IP public sẽ được cấp một IP trong Pool). Khi Remote Users kết nối tới Remote Access Gateway thì IP của Remote Users sẽ được so sánh với dãy IP được định nghĩa sẵn, nếu Source IP của Remote Users có nằm trong IP Pool thì sẽ được cấp.

Việc cấp IP dựa trên source IP sẽ giúp phân biệt giữa Users thường và Users có các quyền đặc biệt.

3.5.2 DHCP

DHCP là phương pháp thứ hai để cấp IP cho Remote Users trong Office Mode. Khi Remote Users kết nối tới Remote Access Gateway thì Remote Access Gateway sẽ gửi request tới DHCP server để cấp IP cho Remote Users. Request gửi tới DHCP server sẽ chứa các thuộc tính

- Host Name
- Fully Qualified Domain Name (FQDN)
- Vendor Class
- User Class

3.5.3 RADIUS Server

RADIUS Server trong Office Mode vừa được dùng để xác thực, vừa dùng để cấp IP.

Cả hai chức năng (xác thực và cấp IP) cần phải chạy trên cùng RADIUS Server.

IP Pool mà RADIUS Server được cấp sẽ được quy định ở Remote Access Gateway.

3.5.4 IP Allocation Order

Thứ tự cấp IP cho Remote Users là từ trên xuống

- Cấp IP theo file *ipassignment. conf.*
- Xác thực và cấp IP theo RADIUS server.
- Sử dụng IP Pool hoặc DHCP Server.

Khi phương pháp cấp IP không được thực hiện thì Remote Access Gateway sẽ xét tới phương pháp thứ hai. Tiếp tục cho đến khi Remote Users có được IP hoặc không cấp được IP (Do hết phương pháp để chọn).

3.5.5 IP pool Versus DHCP

Thông thường việc quản lý IP address và các vấn đề khác đều nằm trên cùng một thiết bị (dễ dàng và nhanh chóng), đó là cấp IP address cho Remote Users qua IP Pool. Tuy nhiên cách đó chỉ hiệu quả đối với những hệ thống nhỏ với số lượng Users ít.

Đối với hệ thống lớn bao gồm nhiều thiết bị khác nhau hay là hệ thống cluster thì DHCP là lựa chọn hiệu quả nhất. Thông qua DHCP, ta có thể quản lý tập trung các IP được cấp cho tất cả các thiết bị gửi yêu cầu tới.

3.6 Optional Parameters

3.6.1 IP Address Lease duration

Sau khi Remote Users được cấp một địa chỉ IP thì IP đó chỉ được sử dụng trong một khoảng thời gian xác định, khoảng thời gian đó gọi là "IP address Lease duration" – Thời gian sử dụng IP.

Remote User sẽ tự động gửi request để làm mới "IP address Lease duration" khi còn phân nửa thời gian sử dụng IP đó

Ví dụ "IP address Lease duration" là 60 phút, thì sau 30 phút thì request làm mới sẽ được gửi, nếu request được chấp nhận và IP được làm mới thì sau 30 phút nữa Remote User mới gửi request làm mới khác. Nếu request không được chấp nhận hoặc thất bại vì một lý do nào đó thì Remote User sẽ tiếp tục gửi khi còn phân nửa thời gian sử dụng (Lần tiếp theo là 15phút, tiếp theo nữa là 7.5 phút, tiếp theo là 3.25 phút…). Nếu sau 60 phút mà IP không được làm mới thì xem như đường kết nối đó kết thúc.

Nếu Remote User muốn sử dụng tiếp đường kết nối thì phải thực hiện tạo kết nối mới, đàm phán IKE…

Nếu IP được cấp nằm trong IP Pool định nghĩa trên Gateway thì "IP Address Lease duration" sẽ do Gateway xác định, mặc định là 15 phút.

Nếu IP do DHCP server cấp thì "IP Address Lease duration" sẽ do DHCP server xác định.

Nếu Remote User ngắt kết nối và tái kết nối tới Remote Access Gateway trong một khoảng thời gian ngắn thì Remote User đó sẽ được cấp cùng một địa chỉ.

3.6.2 WINS and DNS

Để tiện cho việc truy cập của Remote Users vào các host trong mạng Private thì địa chỉ WINS và DNS server sẽ được cấp cho Remote Users.

Thông tin về WINS và DNS server sẽ được gửi tới Remote Users cùng với thông tin và địa chỉ IP.

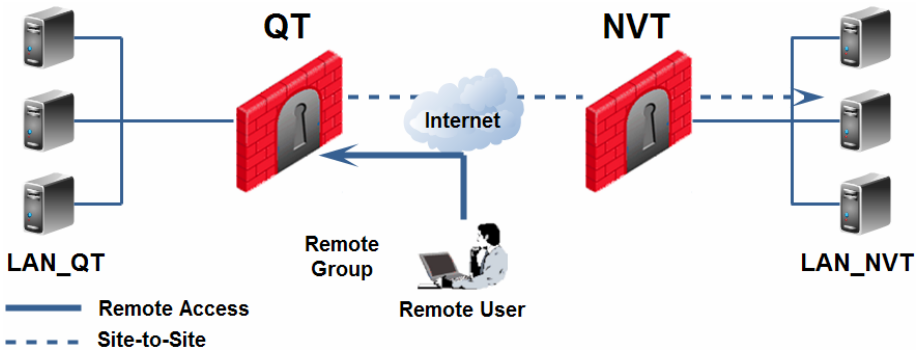
3.7 Office Mode Per Site

Sau khi Remote Users kết nối vào Remote Access Gateway thì Remote Users sẽ được cấp cho Office Mode IP (IP cấp cho Interface ảo). Tất cả các gói tin đi về VPN Domain của công ty sẽ sử dụng Office Mode IP làm source IP.

Cho nên Office Mode IP còn được xem là thuộc VPN Domain (thuộc vùng private của công ty) nếu được cấu hình và có thể tạo kết nối tới vùng Private của một site khác (chi nhánh của công ty).

Tất cả các Gateway cần phải biết Office Mode IP range thì mới sử dụng được chức năng "Office Mode Per Site".

Khi dùng "Office Mode Per Site" thì ta không thể sử dụng chức năng "IP per Users".



Hình A3 – 10 : Office Mode per Site

Như trên hình ta thấy Remote User kết nối Remote Access vào Gateway QT và được cấp Office Mode IP. Do đó Remote User có thể tạo kết nối tới vùng LAN của NVT Gateway (thông qua IPsec VPN Site-to-Site) như là một User trong vùng LAN của QT.

- Gateway QT : VPN Domain = "LAN_QT" + "Remote Group"
- Gateway NVT : VPN Domain = "LAN_NVT"

3.8 IP per user

Trong một số trường hợp, ta cần cấp đúng địa chỉ cho một User nào đó (do sự hạn chế truy cập dịch vụ của Firewall với một số IP hoặc cần cấp những quyền truy cập đặc biệt cho Power Users).

Hai phương pháp giải quyết tốt nhất là dùng DHCP kèm với gán IP cho Users hoặc chỉnh sửa trong file *ipassignment. conf.*

3.8.1 DHCP Solution

Để giải quyết với DHCP, ta làm theo thứ tự như sau

Bước 1: Cấu hình DHCP.

Bước 2: Cấu hình Office Mode sử dụng DHCP để cấp IP.

Bước 3: Ở "MAC address for DHCP allocation" chọn "Calculated per user name".

Bước 4: Install Policy.

Bước 5: Dùng lệnh sau để xem MAC-Addess ứng với IP Addess.

vpn macutil <username>

```
C:\>vpn macutil 070112
DB-DC-24-4F-49-D2, "070112"
```

Bước 6: Trên DHCP server ta cấu hình IP được cấp ứng với MAC-Address đã cho bởi lệnh *macutil.*

3.8.2 *Ipassignment. conf* Solution

Thông qua *Ipassignment. conf* thì ta có thể cấp IP cho từng User. Cấu trúc của file *Ipassignment. conf* bao gồm nhiều dòng, mỗi dòng sẽ có 4 cột chính

Gateway	Type	*IP Address*	***User Name/Group Name***

Ví dụ

QT	*10.200.200.5*	***hiephung***	
QT	addr	*10.200.200.6*	***huutan***
QT	addr	*10.200.1.1*	***CN=admin,CN=users,DC=lotus,DC=vn***
QT	addr	*10.200.1.1*	***CN=admin2,OU=user,O=QT.lotus.vn.sgyw26***
NVT	range	*100.200.10.1 – 100.200.10.120/24*	***VT071***
NVT	net	*10.200.10.32/28*	***Professor***

❖ **Gateway**

Đây là cột định ra tên Gateway sẽ cấp IP cho Users, ta có thể dùng Gateway Name cũng có thể dùng IP Address để định cột **Gateway.**

❖ Type

Là số lượng IP có thể cấp.

- addr : Là địa chỉ xác định. Ví dụ : 10.200.200.5
- range : Là dãy địa chỉ liên tiếp. Ví dụ : *100.200.10.1 – 100.200.10.120/24*
- net : Là một subnet. Ví dụ : *10.200.10.32/28*

❖ *IP Address*

Địa chỉ hoặc dãy địa chỉ được cấp.

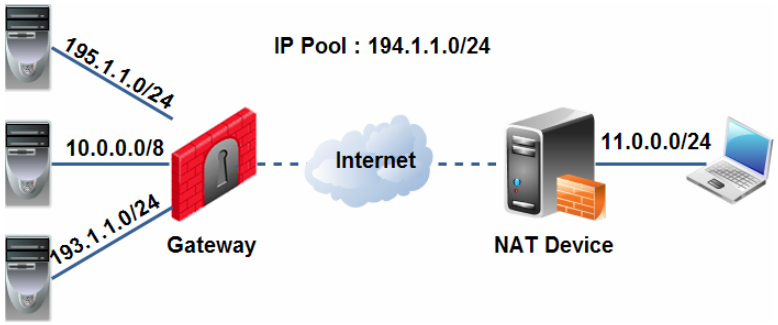
❖ ***User Name/Group Name***

Có thể là username nếu dùng User Name/Group Name hoặc là DN nếu dùng Certificate.

- Certificate cấp bởi LDAP : ***CN=admin,CN=users,DC=lotus,DC=vn***
- Certificate cấp bởi ICA : ***CN=admin2,OU=user,O=QT.lotus.vn.sgyw26***

3.9 Routing Table

3.9.1 Topology Overview



Hình A3 – 11 : Example Topology

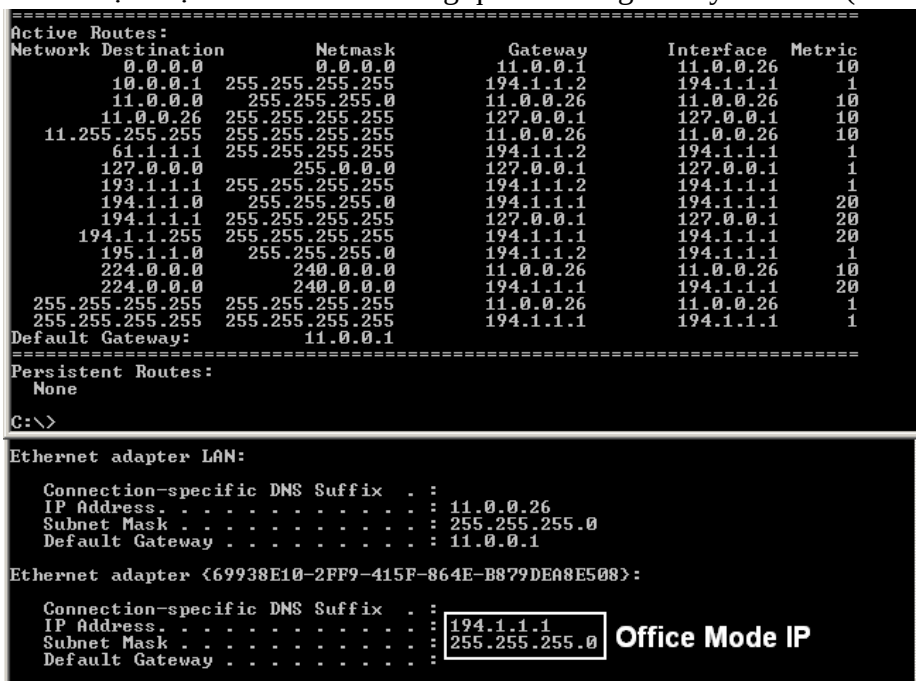
Phía Remote Access Gateway bao gồm

- Management Zone : 193.1.1.0/24
- LAN Zone : 10.0.0.0/8
- DMZ Zone : 195.1.1.0/24 (VPN Domain)
- Office Mode IP Pool : 194.1.1.0/24
- Public IP Addess : 61.1.1.1/24

3.9.2 Routing Table

Sau khi Remote User được cấp IP trong Office Mode IP Pool, đồng thời Remote User cũng sẽ được cấp một bảng Routing để có thể tham gia như một host trong mạng Private. Bất kỳ gói tin nào cũng sẽ được xét theo bảng routing dựa vào Destination của gói tin.

- Nếu Destination của gói tin là thuộc mạng 193.1.1.0/24 – 195.1.1.0/24 – 10.0.0.0/8 – 61.1.1.1/24 thì sẽ được route qua 194.1.1.1 (Metric = 1). Gói tin đi qua cổng Interface ảo sẽ được encapsulate bằng VPN.
- Còn lại được default route thông qua default gateway 11.0.0.1 (Metric = 10).



Hình A3 – 12 : Office Mode Routing Table

Phụ thuộc vào việc quy định VPN Domain ở phía Remote Access Gateway mà bảng routing ở Remote User sẽ được phép đi đến mạng Private nào.

- Theo Topology thì VPN domain là vùng DMZ (195.1.1.0/24) nên trong bảng routing thể hiện là 195.1.1.0/24.
- Các mạng còn lại không thuộc VPN Domain, Remote User chỉ có thể truy cập được vào IP của Remote Access Gateway nên trong bảng routing thể hiện là 193.1.1.1/32 – 10.0.0.1/32 – 61.1.1.1/32.

3.10 SSL Network Extender

3.10.1 Overview

Khi Remote Users kết nối tới công ty, ngoài đường truyền cần được bảo vệ thì còn những yêu cầu đặc biệt khác cần được đáp ứng ở Remote Users như

- Connectivity – Tính kết nối : Các kết nối từ Remote Users tới công ty có thể xuất phát từ nhiều nơi khác nhau (Sau Firewalls, NAT devices, Proxies…) với những yêu cầu về dịch vụ được đáp ứng khác nhau (Mail, Web, File Sharing…). Do đó đường truyền Remote Access cần đáp ứng đủ các yêu cầu đó mà không bị hạn chế bởi các thiết bị mạng phía Remote Users (Restricted Internet Access).

- Secure Connectivity – Tính an toàn kết nối : Đảm bảo tính an toàn cho dữ liệu được truyền, xác thực Remote Users, xác thực Remote Access Gateway và xác thực dữ liệu được truyền.
- Usability – Tính dễ dàng sử dụng : Dễ dàng cài đặt, không đòi hỏi Remote Users phải có kiến thức nhiều về mạng cũng như máy tính mới sử dụng được Remote Access.

3.10.2 Checkpoint Solution – SSL Network Extender

Khi sử dụng SNX thì phía client sẽ tải và cài đặt một chương trình ActiveX, và dựa trên chương trình đó kết nối tới Remote Access Gateway trên nền giao thức SSL (Quá trình tải, cài đặt và cấu hình hoàn toàn tự động).

Phần cấu hình sẽ nằm hoàn toàn về phía Remote Access Gateway, lúc này đóng vai trò như một SSL Web Server, cho nên việc quản lý các bước cấu hình sẽ được dễ dàng và tập trung.

SNX làm việc dựa trên Remote Access VPN, Office Mode và Visitor Mode. Khi Remote Users kết nối vào Remote Access Gateway thì Remote Users sẽ tải và cải đặt một chương trình ActiveX, qua đó trình duyệt được xem như là chương trình SecureClient/SecuRemote và được cấp IP trong Office Mode IP Pool.

Để tăng thêm tính bảo mật thì SNX còn có cơ chế Endpoint Security on Demand (ESOD) sẽ quét máy Remote Users để kiểm tra các phần mềm độc hại trước khi cho phép Remote Users tham gia vào mạng nội bộ.

Do quá trình quản lý SecurePlatform cũng thông qua nền SSL(443) nên khi sử dụng SNX trên nền SecurePlatform có thể xảy ra xung đột giữa SNX và cổng quản lý thiết bị (Management Portal). Để tránh trường hợp này ta có thể linh hoạt thay đổi cổng quản lý bằng hai cách sau

- Thay đổi port truy cập vào cổng quản lý. `webui enable <portnumber>`
- Tắt cổng quản lý. `webui disable`

3.11 Clientless VPN

3.11.1 Overview

Ngoài những yêu cầu cần được đáp ứng đã nêu ra ở phần SSL Network Extender, thì Remote Users còn có thể rơi vào một số trường hợp đặt biệt

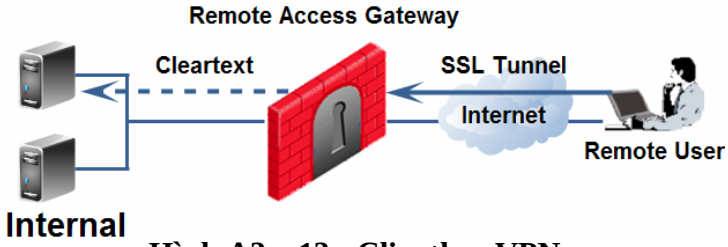
- Remote Users sử dụng máy tính công cộng với quyền hạn sử dụng rất hạn chế, không được phép cài đặt chương trình, phần mềm, không được cài ActiveX hoặc Java Runtime.
- Những Internal server dành cho Remote Users cần được bảo vệ đường truyền và giám sát, lọc những traffic có hại.

Đáp ứng yêu cầu đó thì Checkpoint đưa ra giải pháp Clientless VPN.

3.11.2 Checkpoint Solution – Clientless VPN

Với Clientless VPN

- Remote Users kết nối tới Internal Server một cách an toàn thông qua các giao thức mã hóa mà không cần cài đặt bất kỳ phần mềm, chương trình nào.
- Cung cấp khả năng giám sát dữ liệu vào ra ở Remote Access Gateway.
- Xác thực Remote Users và Remote Access Gateway.
- Sử dụng các thuật toán mã hóa mạnh như 3DES.



Hình A3 – 13 : Clientless VPN

3.11.3 Workflow

Quá trình tạo kết nối từ Remote Users tới Internal server sẽ trải qua hai giai đoạn

3.11.3.1 Establishing a Secure Channel

- Remote User gửi HTTPS request tới Internal server (qua NAT hoặc trực tiếp).
- Request đi qua Gateway, Gateway kiểm tra trong các Policy, nếu request thỏa với Policy cho phép HTTPS thì request được xử lý.
- Gateway sẽ tạo kết nối Clientless VPN cho Remote User và gửi request tạo kết nối cleartext (kết nối HTTP) tới Internal server. Như vậy kết nối từ Remote User đến Internal server sẽ được quản lý bởi Gateway.
- Kết nối Clientless VPN từ Gateway tới Remote User là kết nối an toàn HTTPS (SSL) và sử dụng Certificate của Gateway.

3.11.3.2 Communication Phase

- Gateway tạo kết nối cleartext tới Internal server. Như vậy toàn bộ kết nối của Remote User đến Internal server đều thông qua Gateway và được quản lý bởi Gateway.

Do kết nối từ Gateway tới Internal server là cleartext cho nên Gateway hoàn toàn có thể kiểm tra traffic đi qua lại giữa Remote User và Internal server.

Theo khía cạnh của Remote Users thì Remote Users kết nối trực tiếp tới Internal Server thông qua SSL, nhưng thật tế kết nối SSL đó là với Gateway.

3.11.4 Clientless VPN Consideration

3.11.4.1 Certificate Presented by the Gateway

Certificate đại diện cho Gateway sẽ được gửi cho Remote User trong quá trình xác thực Gateway. Remote User sẽ xác định danh tính của Gateway thông qua

Certificate để đảm bảo mình kết nối tới chính xác Gateway. Như vậy Certificate đó phải đảm bảo được ký bởi một trusted CA (Như của Verisign).

Tuy nhiên trong một số trường hợp, Gateway sử dụng ICA để cấp Certificate, cho nên để Remote User có thể xác minh tính chính xác của Certificate thì Remote User phải tải Certificate của ICA từ Gateway về.

3.11.4.2 Number of Internal Servers to Run

Để quản lý tốt được các kết nối của Remote Users, thì tốt nhất chỉ tạo kết nối tới 10 Internal servers khác nhau (Với 150 Users cho mỗi Internal server) trên mỗi Gateway.

4 Remote Access Routing

4.1 Overview

Trong một số trường hợp thì Remote User sẽ không thể kết nối trực tiếp tới Remote User (hoặc Gateway) khác. Ví dụ

- Remote Users sử dụng các dịch vụ peer-to-peer như là VoIP, Microsoft NetMeeting cần kết nối trực tiếp với nhau. Tuy nhiên các Remote Users không thể kết nối trực tiếp với nhau.
- Remote Users được phép kết nối tới Headquarters Gateway, nhưng dữ liệu cần sử dụng lại nằm ở Branch's VPN Domain.

Từ đó đặt ra vấn đề là cần tăng khả năng Routing của hệ thống để Remote User có thể giao tiếp với Remote User (hoặc Gateway) khác.

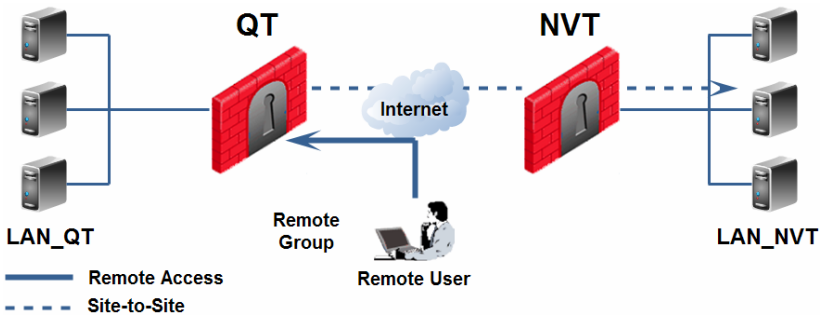
4.2 Checkpoint Solution – Hub Mode

Giải pháp của Checkpoint là cho phép Remote Users được phép kết nối của Remote Users được phép route trực tiếp tới Remote Access Gateway. Như vậy toàn bộ các kết nối của Remote Users đều được giám sát bởi Remote Access Gateway.

Khi sử dụng Hub Mode thì phải sử dùng đồng thời Office Mode. Vì IP address của Remote Users sẽ hỗ trợ khả năng route hoàn chỉnh. Office Mode giúp việc quản lý Remote Users sẽ được dễ dàng và bảo mật hơn thông qua Office Mode IP Pool.

4.3 Hub Mode Situation

4.3.1 Remote User to Another VPN Domain



Hình A3 – 14 : Hub Mode – Remote User to Another VPN Domain

Trường hợp đặt ra là Remote User cần kết nối tới mạng LAN_NVT sau Gateway NVT. Tuy nhiên Gateway NVT không hỗ trợ chức năng Remote Access cho Remote User. Để giải quyết trường hợp này, thì Remote User có thể kết nối tới LAN_NVT thông qua Gateway QT.

- Remote User kết nối Remote Access tới Gateway QT.
- Tạo kết nối Site-to-Site giữa Gateway QT và Gateway NVT.
- Cấu hình Office Mode IP Pool thuộc VPN Domain.
- Tất cả Request của Remote User được gửi đến Gateway QT.
- Gateway QT dựa vào bảng route đưa request tới đúng đích đến.

Kết nối từ Remote Users tới Gateway QT là kết nối Remote Access, kết nối từ Gateway QT tới Gateway NVT là Site-to-Site.

4.3.2 Remote User to Remote User

Trường hợp đặt ra là Remote Users sử dụng các dịch vụ peer-to-peer như là VoIP, Microsoft NetMeeting cần kết nối trực tiếp với nhau. Như vậy ta có thể kết nối hai Remote Users trực tiếp với nhau với Hub Mode thông qua hai cách

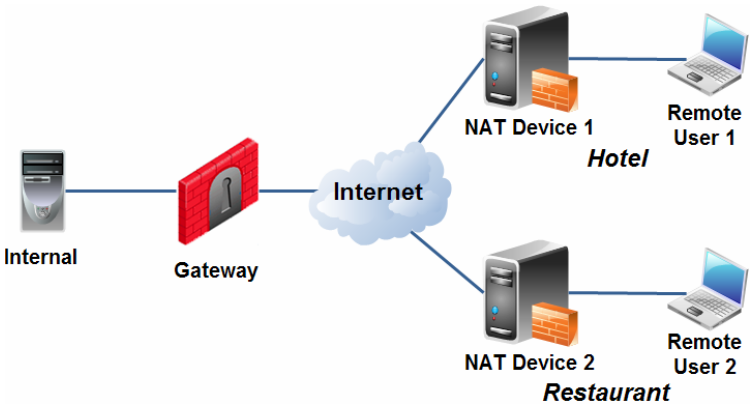
- ❖ Route tất cả các traffic đi qua Gateway.
- ❖ Đưa Office Mode IP Pool vào VPN Domain.

4.3.2.1 Remote Users at the same Gateway

Trong trường hợp này thì tất cả traffic của Remote Users sẽ đổ về cùng một Gateway, Gateway sẽ route và đưa traffic đến đúng địa chỉ đích. Trường hợp có thể không cần sử dụng Office Mode.

Đường kết nối từ Remote User 1 tới Remote User 2 vẫn đảm bảo là kết nối an toàn (IPsec VPN).

Tuy nhiên việc quản lý Remote User khá phức tạp và kém bảo mật.

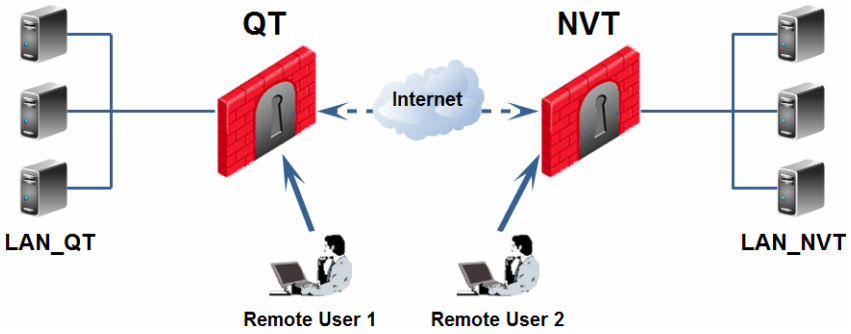


Hình A3 – 15 : Hub Mode – Remote User at the same Gateway

4.3.2.2 Remote Users at different Gateways

Trong trường hợp này thì thứ tự tạo kết nối sẽ được thực hiện như sau

- Remote User 1 tạo kết nối Remote Access tới Gateway QT.
- Remote User 2 tạo kết nối Remote Access tới Gateway NVT.
- Traffic của User 1 sẽ được Gateway QT route và đưa qua Gateway NVT.
- Gateway NVT sẽ đẩy traffic của Remote User 1 cho Remote User 2.



Hình A3 – 16 : Hub Mode – Remote Users at the different Gateway

Điều kiện để Remote User 1 và Remote User 2 có thể kết nối với nhau

- Cần sử dụng Office Mode.
- Office Mode IP Pool của cả hai Gateway sử dụng cần phải được định nghĩa ở trên hai Gateway.
- Office Mode IP Pool của hai Gateway không được phép trùng nhau – Overlapping.

4.3.3 Remote User to Internet Server

Đây là trường hợp này phát sinh cho Remote Users khi sử dụng Hub Mode.

Do tất cả các traffic của Remote Users đều được route về Remote Access Gateway, nên khi Remote Users cần truy cập vào một server ở ngoài Internet, thì request của Remote Users sẽ không trực tiếp tới server đó mà cũng sẽ thông qua Remote Access Gateway. Mặc khác Source IP của request nằm trong dãy Private Address, nên phía server không thể respond về cho Remote Users.

Để giải quyết trường hợp này thì cần sử dụng Office Mode kết hợp với NAT dãy Office Mode IP Addess. Remote Access Gateway sẽ phải NAT rồi gửi request tới server. Nếu Remote Access Gateway không hỗ trợ NAT cho Office Mode IP Pool thì coi như kết nối của Remote Users thất bại.

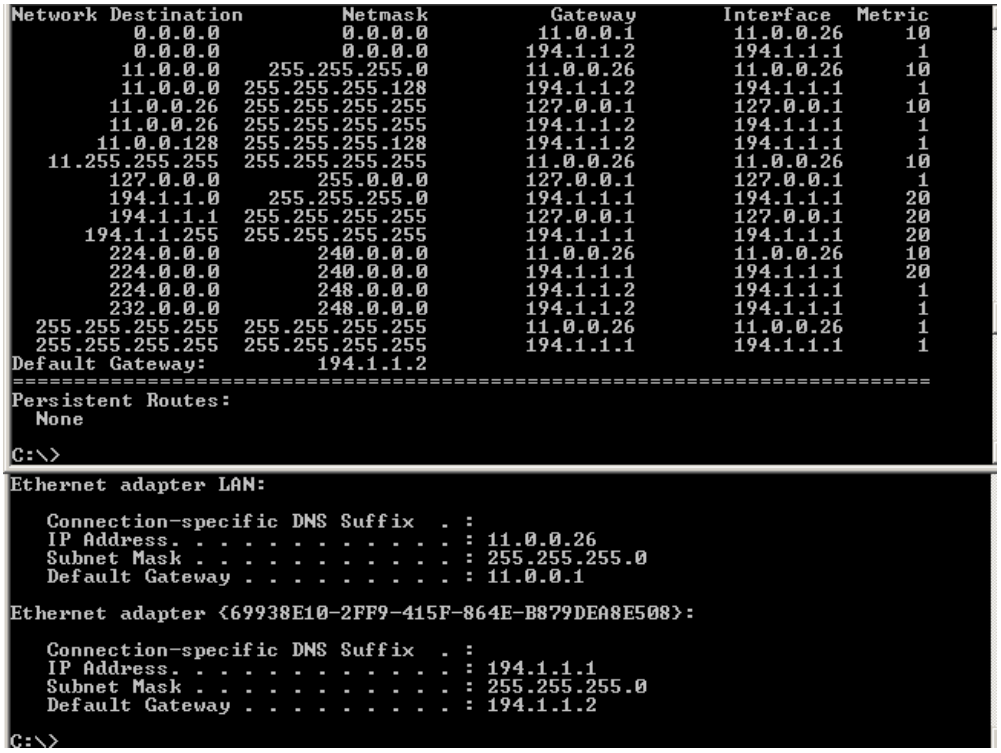
Lý do cần sử dụng Office Mode ở đây là vì khi NAT thì dãy địa chỉ được NAT cần phải cố định, mà Remote Users lại có địa chỉ thay đổi liên tục.

4.4 Hub Mode Routing Table

Phía Remote Access Gateway bao gồm ba mạng Private, một IP Public và Office Mode IP Pool

- Management Zone : 193.1.1.0/24
- LAN Zone : 10.0.0.0/8
- DMZ Zone : 195.1.1.0/24 (VPN Domain)
- Office Mode IP Pool : 194.1.1.0/24
- Public IP Addess : 61.1.1.1/24

Tương tự như Routing Table của Office Mode, tuy nhiên ở Hub Mode còn có thêm một đoạn Default Route với Next hop là trỏ về Remote Access Gateway với Metric = 1. Như vậy toàn bộ traffic sẽ đi về Gateway dù là traffic về VPN Domain hay ra Internet.



Hình A3 – 17 : Office Mode Routing Table

CHAPTER 02 – IPS INTRUSION PREVENTION SYSTEM

Trong chapter này ta sẽ nói về hệ thống IPS – Intrusion Prevention System cùng các quy tắc hoạt động và công nghệ của IPS.

Bên cạnh đó là phân tích các dạng Signature của IPS.

Cuối cùng là giải pháp IPS của Checkpoint

Chapter 02 – Endpoint Security bao gồm hai phần

- *IPS Overview*
- *Checkpoint Solutions*

❖ IPS Overview

Trong phần EPS Overview ta sẽ giới thiệu tổng quan về cấu trúc, phân loại IPS.

Các dạng Signature của IPS.

- IPS – IDS Overview
- NIPS – Network-based Intrusion Prevention System
- HIPS - Host-based Intrusion Prevention System
- HIPS and NIPS Comparision
- IPS Signature

❖ Checkpoint Solution

Trong phần này ta sẽ nói về các giải pháp của Checkpoint, các tùy chọn và cách cấu hình Checkpoint IPS.

Các giải pháp tối ưu hóa IPS của Checkpoint.

- Checkpoint IPS Overview
- Checkpoint IPS Profile
- Checkpoint IPS Protection
- IPS Optimization

A . IPS Overview

Trong môi trường internet, các đoạn mã độc hại được phát tán một cách nhanh chóng và xuyên suốt trong hệ thống mạng của cả thế giới. Do đó bất cứ hệ thống mạng nào cũng phải được chuẩn bị để có khả năng nhận biết nhanh chóng sự nguy hiểm và làm giảm thiểu mức độ ảnh hưởng của các cuộc tấn công này hay còn gọi là hệ thống bảo vệ thời gian thực (Realtime Protection).

Các công nghệ phát hiện nhận dạng mã độc đã được áp dụng vào mô hình kiến trúc hệ thống mạng từ rất sớm như IDS (Intrusion Detection System), tuy nhiên sau một thời gian sử dụng, sự thiếu hiệu quả trong quá trình làm việc của IDS liên tục bị khai thác triệt để, vì thế một phương thức làm việc mới đã được ra đời để khắc phục các nhược điểm của IDS. Thay vì chỉ trực quan bắt gói kiểm tra sau đó mới có biện pháp gửi yêu cầu đến các thiết bị quản lý trong hệ thống để có hướng xử lý thích hợp, thì những gói tin đó có thể đã đến được endpoint. Phương thức chặn gói kiểm tra và đưa ra biện pháp xử lý ngay được áp dụng, với phương thức này, ta có thể giảm một lượng lớn các cuộc tấn công và hiệu quả hơn so với IDS, và phương pháp này còn gọi là IPS (Intrusion Prevention System). Tuy nhiên, phương thức mới này đòi hỏi công việc xử lý nhiều hơn nên ít nhiều đều ảnh hưởng đến hiệu năng của cả hệ thống. Vì thế, vai trò của những nhà quản trị có ảnh hưởng rất lớn, họ phải nắm rõ hệ thống mình quản lý để đưa ra những policy thích hợp nhằm tối ưu hệ thống được quản lý…

1 Overview

1.1 IPS vs IDS

IPS là một thiết bị (appliance) cũng có thể là một ứng dụng (application). Với phương thức hoạt động của IDS ngày càng lỗi thời và dễ dàng bị khai thác, IPS là một sự phát triển dựa trên IDS, bổ xung khắc phục những hạn chế của IDS nhằm tăng cường khả năng bảo mật cho hệ thống. Nếu nói IDS là một hệ thống mang tính thụ động, thì IPS sẽ được xem là một hệ thống mang tính chủ động toàn diện với khả năng kiểm tra, phát hiện, hạn chế, ngăn chặn những cuộc tấn công ngay từ ban đầu (so với việc bỏ qua dữ liệu đầu tiên của kết nối, sau đó mới thông báo về tính vi phạm của kết nối đó khi phát hiện).

- Khả năng phân tích

  Với cơ chế quét theo stream (stream là dạng traffic được tập hợp bởi nhiều packet do kích thước quá lớn nên được chia nhỏ ra để truyền đi trên mạng), các attacker sẽ không thể lợi dụng phương thức chèn các đoạn mã độc vào các gói tin có payload lớn, nếu IPS/IDS phát hiện gói tin đó là một dạng gói tin được chia nhỏ, thì nó sẽ tập hợp đầy đủ các gói thành một payload hoàn chỉnh rồi bắt đầu tiến hành quét. Với phương pháp quét này, dẫn đến nhược điểm là gây ảnh hưởng đến độ trễ cũng như hiện tượng mất gói do cờ timer của mỗi gói tin.

- Khả năng tìm kiếm

  Hạn chế về mặt tìm kiếm của IDS chính là khả năng bắt gói, vai trò của IDS chỉ là một thiết bị giám sát, xử lý những bản sao của gói tin từ Firewall gửi đến. Do đó tính sẵn sàng của IDS không cao vì đối với mỗi kết nối, hoặc cuộc tấn công nào đó, ở gói tin đầu tiên IDS cần phải nhận bản sao của gói tin đó từ Firewall rồi mới tiến hành phân tích, trong thời gian phân tích bản sao đó, thì gói tin chính đã đi tới endpoint. Điều này

dẫn tới việc IDS sau khi phát hiện dấu hiệu bất thường rồi mới báo cho các thiết bị quản lý thực hiện việc loại bỏ kết nối đó trong khi endpoint đã xử lý gói tin đầu tiên và bị ảnh hưởng, sự bảo vệ này không triệt để. Để khắc phục điểm yếu này, IPS được quản lý traffic ra và vào mạng được bảo vệ, mọi dữ liệu di chuyển ra và vào mạng được bảo vệ đều được IPS chặn lại kiểm tra, sau đó mới đưa ra hành động tương ứng. Điều này giúp ngăn chặn các cuộc tấn công hoặc mối nguy hiểm ngay từ đầu.

- Hành động đáp trả

IDS chỉ thực hiện nhiệm vụ giám sát và gửi thông báo, không trực tiếp tham gia vào quá trình ngăn chặn, để nâng cao độ bảo mật và tính sẵn sàng, IPS được lập trình sẵn các chức năng có thể hành động đáp trả độc lập khi phát hiện ra những dấu hiệu bất thường, độ bảo mật được nâng cao hơn.

1.2 Terminology

- True Positive : Chỉ ra sự phát hiện và hành động ngăn chặn của IPS về một tình huống có thể khiến hệ thống bị tấn công và phát hiện đó là chính xác. (Phát hiện một stream dữ liệu chứa mã độc, IPS tiến hành loại bỏ phiên kết nối này).
- True Negative : Chỉ ra khả năng IPS không thể phát hiện ra một tình huống tấn công.
- False Positive : Chỉ ra khả năng IPS xác định được tình huống đó gần giống với một tình huống tấn công, nhưng không chính xác là một cuộc tấn công. Tuy nhiên IPS vẫn xem đó là một cuộc tấn công.
- False Negative : Chỉ ra khả năng IPS không thể phát hiện ra một tình huống tấn công.

2 Classification

2.1 NIPS – Network-based Intrusion Prevention System

NIPS là một thiết bị phần cứng hoặc một dạng phần mềm được tích hợp (IOS Cisco) thường được đặt làm Gateway của mạng được bảo vệ, kiểm tra lượng traffic lưu thông qua NIPS để đảm bảo an toàn cho hệ thống do NIPS quản lý.

- Chức năng

NIPS được thiết kế để bảo vệ kiến trúc hệ thống mạng, lọc dữ liệu ngay từ ban đầu của kết nối, giảm thiểu các trường hợp bị tấn công ngay từ thời điểm đầu.

- Hoạt động

Thường được đặt ở những vị trí vành đai giữa hai mạng, đóng vai trò như một Gateway, xử lý tất cả các dữ liệu traffic. Khi gói tin đi qua thiết bị này sẽ được chặn lại, sử dụng các phương thức kiểm tra để có những hành động đáp trả thích hợp.

- Ưu điểm

NIPS là một dạng mô hình quản lý các dữ liệu được truyền ra vào hệ thống mạng được bảo vệ, giúp nhà quản trị dễ dàng kiểm tra quản lý hệ thống mạng. Bằng những cảnh báo được gửi tới nhà quản trị khi hệ thống có những sự kiện bất thường xảy ra,

như phân vùng đang bị tấn công, lưu lượng traffic bất thường… Đồng thời tạo log ghi nhận các dấu hiệu này.

Đều đặc biệt, hệ thống NIPS này được xây dựng xử lý những dữ liệu traffic được bảo vệ, và không tham gia vào các dịch vụ định tuyến traffic như các thiết bị mạng khác chạy trên chính hệ điều hành riêng cho NIPS, không bị hạn chế bởi yếu tố xung đột hệ thống do đòi hỏi tính tương thích khi cài lên một hệ thống khác. Quản lý dạng tập trung, đơn giản.

Không thể phát hiện ra sự hiện diện của thiết bị NIPS trong hệ thống mạng.

Về khả năng xử lý, do NIPS đòi hỏi đó là những thiết bị đặc trưng riêng và có nhiệm vụ độc lập nên tốc độ xử lý rất cao.

Các thành phần cần có của NIPS

- Network Interface Card (NIC) : Dùng để kết nối vào hệ thống mạng.
- Processor : Bộ xử lý được xây dựng hỗ trợ các chức năng phân tích và so sánh để xác định loại tấn công hoặc hành vi tấn công.
- Memory : Lưu trữ các cơ sở dữ liệu tạm thời dùng trong các hoạt động của IPS cũng như làm bộ đệm để chức các traffic dạng streaming.

❖ Nhược điểm

Những nhược điểm lớn của hệ thống này chính là độ trễ, sự không ổn định về hiệu năng của hệ thống mạng. Đối với các traffic được mã hóa (dùng trong VPN, SSL…) thì các thiết bị IPS sẽ bỏ qua, và khi đến endpoint thì các gói tin chứa mã độc sẽ được giải mã và thực thi. Tuy nhiên nếu endpoint bị nhiễm mã độc và gây ra những hành động bất thường đối với hệ thống mạng (có thể lưu lượng traffic từ endpoint đó sẽ tăng đột ngột) thì NIPS vẫn nhận ra và đưa ra những biện pháp xử lý thích hợp.

Một nhược điểm khác là nếu payload của một traffic quá lớn thì nó sẽ được chia nhỏ ra, vì thế thiết bị NIPS sẽ không gửi đi ngay sau khi nhận những gói tin đầu mà sẽ tập hợp các gói tin lại và nối lại thành payload hoàn chỉnh để kiểm tra, sau đó mới có hướng xử lý tiếp theo, do đó nguyên hệ thống (CPU, Ram…) của thiết bị NIPS sẽ bị chiếm dụng, đồng nghĩa với việc giá thành để xây dựng cho một hệ thống NIPS sẽ rất lớn và độ không ổn định của hệ thống mạng sẽ tăng cao nếu các thiết bị này bị quá tải, đôi khi dẫn đến sự không ổn định của hệ thống mạng. Và với mô hình NIPS thì không thể đảm bảo được các cuộc tấn công đã được ngăn chặn thành công hay không.

2.2 HIPS – Host-based Intrusion Prevention System

HIPS : Là một phần mềm đuợc cài trực tiếp trên endpoint cần được bảo vệ. Việc bảo vệ này chỉ mang tính chất nội bộ.

❖ Chức năng

HIPS cung cấp các chức năng : Confidentality, Integrity, Availability cho dữ liệu và hệ thống của endpoint (Servers, Desktops, Laptops…). HIPS hoạt động dựa vào sự kết hợp giữa công nghệ phân tích dựa theo hành động và các mẫu được định nghĩa sẵn (Signature-based) để phát hiện ra các dấu hiệu bất thường có thể gây ảnh hưởng đến hệ thống endpoint. Cơ sở dữ liệu của HIPS được update thường xuyên (thông qua một

server) giúp cho khả năng bảo vệ tăng cao và an toàn cho endpoint trước những mối đe dọa mới. HIPS thường được tích hợp các chức năng của các chương trình Anti-virus, Firewall.

❖ Hoạt động

HIPS sẽ can thiệp vào hoạt động của các application, khi application thực hiện một tiến trình truy xuất hoặc yêu cầu hệ thống cung cấp tài nguyên hệ thống để thực thi, dựa vào cơ chế phân tích của mình, HIPS tiến hành các hình thức kiểm tra và đưa ra hành động đáp trả hợp lý.

❖ Ưu điểm

Ưu điểm lớn của hệ thống HIPS là tính bảo vệ toàn diện, nó sẽ dễ dàng phát hiện và ngăn chặn các cuộc tấn công đến endpoint đó, bảo vệ các tài nguyên hệ thống của endpoint. Khắc phục nhược điểm của NIPS là xử lý được các traffic bị mã hóa, do sau khi endpoint nhận được traffic sẽ thực hiện quá trình giải mã, ngay sau khi traffic được giải mã và được application thực thi, lúc đó dữ liệu sẽ được HIPS kiểm tra và đưa ra hành động. Xử lý các traffic có payload lớn tốt hơn do xử lý dạng nội bộ, chỉ xử lý các traffic của host đó nên độ trễ cũng như sự ổn định của hệ thống mạng không bị ảnh hưởng. Từ đó có thể xác định được hệ thống có đang bị tấn công hay không.

❖ Nhược điểm

Do HIPS chỉ bảo vệ nội bộ, nên với mô hình này, các nhà quản trị sẽ gặp khó khăn trong việc quản lý hệ thống mạng của mình, bao gồm việc cập nhật cơ sở dữ liệu của HIPS, việc cài đặt cũng như linh hoạt trong việc bảo vệ, và khắc phục các lỗi do HIPS gây ra (một số trường hợp HIPS có thể xóa cả tập tin hệ thống…). Đồng thời yêu cầu phải có sự tương thích với hệ thống máy endpoint, nếu không có thể dẫn đến tình trạng không tương thích và hoạt động không ổn định. Không thể quản lý các traffic trong hệ thống mạng, do đó không thể ngăn chặn triệt để nguồn gốc của các cuộc tấn công.

2.3 Comparision

❖ Ưu điểm

HIPS	NIPS
- Xử lý được dữ liệu bị mã hóa. - Bảo vệ mang tính cục bộ, độ chính xác cao và dễ dàng phát hiện được khi bị tấn công. - Không ảnh hưởng tới hệ thống mạng (độ trễ, mất gói…).	- Là một thiết bị hoặc một phần mềm được tích hợp. - Khó xác định sự tồn tại của NIPS trong hệ thống. - Mang tính tương thích cao, do được thiết kế trên hệ thống riêng (hardening). Nâng cao khả năng xử lý. - Có thể kiểm soát và quản lý được tình trạng hệ thống mạng. - Mang tính tập trung.

❖ **Nhược điểm**

HIPS	NIPS
- Là một phần mềm, được cài đặt trên endpoint. Đòi hỏi tính tương thích với hệ điều hành của endpoint. Khó đạt được hiệu suất tối ưu. - Không thể biết được tình trạng của hệ thống mạng. - Khó quản lý tập trung trong việc cài đặt, cập nhật, sửa chữa lỗi. - Có thể bị attacker phát hiện sự tồn tại. - Chỉ bảo vệ cho một endpoint đơn lẻ. Không ngăn chặn triệt để nguồn gốc của các cuộc tấn công.	- Không thể xử lý những dữ liệu mã hóa. - Khó đảm bảo được ngăn chặn hoàn toàn những cuộc tấn công. - Gây ảnh hưởng tới tính ổn định của hệ thống mạng như độ trễ, mất gói…

3 IPS Signature

3.1 Signature Definition

IPS signature định nghĩa những quy luật, nguyên tắc mà IPS sẽ dựa vào đó để xác định một gói tin, hoạt động hoặc một sự kiện nào đó có được xem là bất thường hay không và có những hành động đáp trả hợp lý.

❖ Bao gồm

- Signature-based : Các loại cơ sở dữ liệu.
- Signature types : Kiểu phân tích dữ liệu.
- Signature trigger : Phương thức xác định một hành động.
- Signature action : Hành động đáp trả.

3.2 Phân loại Signature

3.2.1 Signature-based

Signature-based là dạng cơ sở dữ liệu bao gồm các dấu hiệu để xác định một đoạn mã hoặc một hành động là bất thường. Có các dạng cơ sở dữ liệu sau

- Exploit-based : Bao gồm các dấu hiệu, các đoạn mã của các loại virus, worm,…
- Vulnerability-based : Bao gồm thông tin về các lỗ hổng của các hệ thống, chương trình thường bị lợi dụng để tấn công.
- Behavior-based : Bao gồm các định nghĩa về các hoạt động được xem là bất thường, bất hợp pháp.

- Profile-based : Bao gồm các định nghĩa về các hoạt động được xem là bình thường của một hệ thống tại một thời điểm nào đó (thời điểm tạo ra profile).

Signature-based được chia làm hai loại là

- ❖ Statistical Analysis - Cơ sở dữ liệu phân tích chính xác.
- ❖ Heuristic Analysis - Cơ sở dữ liệu phân tích dựa theo hành động.

3.2.1.1 Statistical Analysis

Gồm Exploit-based và Vulnerability-based, để có được những cơ sở dữ liệu theo dạng này, đòi hỏi cần phải có một quá trình phân tích sâu vào cách thức hoạt động của các giao thức được sử dụng, nắm rõ về các ngôn ngữ lập trình, hiểu biết về hệ thống để có khả năng phân tích, đọc hiểu các đoạn mã độc và xác định các thức xử lý đối với từng loại mã độc.

3.2.1.2 Heuristic Analysis

Gồm Profile-based, Behavior-based, để có những cơ sở dữ liệu theo dạng này, đòi hỏi phải có sự phân tích tổng thể, tìm ra cái chung nhất giữa các loại hoạt động, để có thể nhận biết được sự khác biệt giữa các hành động bình thường và bất bình thường.

3.2.2 Signature types

Một hệ thống IPS hiệu quả làm việc tốt, ngoài việc có một cơ sở dữ liệu đầy đủ về các loại tấn công, dấu hiệu vi phạm, thì yếu tố góp phần quan trọng nhất chính là hình thức kiểm tra phân tích traffic. Một cơ sở dữ liệu đầy đủ mà hình thức kiểm tra kém hiệu quả thì vẫn không đạt được hiệu quả như mong muốn. Signature types bao gồm hai loại

3.2.2.1 Atomic Signature

Atomic Signatures là dạng đơn giản nhất, hình thức kết hợp giữa phương thức kiểm tra và cơ sở dữ liệu để xác định hành động bất hợp pháp hay hợp pháp chỉ dựa vào một gói tin, sự kiện nào đó. Không cần phải duy trì trạng thái, thông tin các gói tin hoặc kết nối đó, không cần quan tâm đến thời điểm trước và sau của các gói tin này, Atomic signature chỉ đơn giản khi tiếp nhận một gói tin, dùng cơ chế kiểm tra, dựa vào những dấu hiệu, thông tin trong Signature-based của mình để kiểm tra, và việc kiểm tra sẽ kết thúc trong một quá trình, sau khi gói tin được đi qua IPS thì mọi thông tin về gói tin đó sẽ được xóa bỏ.

- ❖ Ưu điểm

Do không thực hiện các cơ chế lưu trữ thông tin trạng thái, nên không chiếm dụng nhiều bộ nhớ, do đó việc định rõ các Signature-based giúp cho hệ thống IPS dễ phát hiện được nguyên nhân và khắc phục.

- ❖ Nhược điểm

Số lượng Signature-based sẽ vô cùng lớn, do phương thức này đòi phải có những thông tin về những dấu hiệu của các hoạt động, gói tin bất thường và các gói tin bất thường đó phải được gửi đi dưới dạng Non-fragmented, do Atomic chỉ hỗ trợ kiểm tra theo dạng từng gói tin.

Do sự không linh hoạt trong việc thiết lập cơ chế lưu giữ trạng thái, dẫn đến tỉ lệ cảnh báo False Positive cao, thậm chí False Negative vì các mã độc hoàn chỉnh không chỉ luôn luôn chứa trong một gói tin, nó có thể được phân phối đều các đoạn mã vào nhiều gói tin khác nhau, với hình thức quét theo gói của Atomic thì các attacker dễ dàng qua mặt được hệ thống.

Do lượng Signatures ngày càng nhiều, quá trình xử lý cũng nhiều hơn (một phần do không có cơ chế lưu trữ trạng thái nên việc kiểm tra phải thực hiện nhiều lần đối với nhiều gói của một payload), và ảnh hưởng tới hiệu suất của hệ thống.

3.2.2.2 Stateful Signature

Stateful Signature là một dạng quét theo stream, Stateful Signature sẽ tiến hành tái tạo lại toàn bộ payload của một tập tin hay dữ liệu được truyền qua mạng, sau đó tiến hành kiểm tra dấu hiệu và hoạt động của payload này để có biện pháp xử lý thích hợp. Do phải duy trì những thông tin, trạng thái của các gói tin đi qua nó trong bộ nhớ của hệ thống, nên mỗi Signature phải được định nghĩa một khoảng thời gian để duy trì thông tin về các traffic của sự kiện đó nhằm hạn chế tình trạng Out-of Memor.

- Ưu điểm

Với khả năng duy trì trạng thái các traffic, Stateful dễ dàng khắc phục được nhược điểm chỉ có thể quét theo gói của Atomic. Bằng cách lưu trữ, tập hợp đầy đủ những thông tin của các gói dữ liệu đi qua nó, nên khi IPS phát hiện gói tin nào được chia thành nhiều phần do độ dài quá lớn, IPS sẽ tổng hợp các gói tin lại thành gói hoàn chỉnh và tiến hành kiểm tra và đưa ra hành động đáp trả thích hợp.

- Nhược điểm

Nhược điểm lớn nhất của hình thức này là khả năng duy trì trạng thái traffic được kiểm tra. Do quá trình duy trì trạng thái này sẽ chiếm bộ nhớ và khả năng xử lý của IPS, nên hiệu suất của hệ thống IPS sẽ giảm đáng kể (Độ trễ, mất gói…) nếu IPS phải xử lý quá nhiều traffic cùng thời điểm.

3.2.3 Signature trigger

Các phương thức phân tích, kiểm tra các dấu hiệu bất thường chính là cốt lõi của hệ thống IPS. Có những phương thức đơn giản và cũng có những phương thức với cơ chế thực hiện vô cùng phức tạp. Hầu hết các hệ thống IPS trên thế giới đều sử dụng chung các tiêu chuẩn này để có thể kiểm soát, quản lý traffic của endpoints hoặc toàn hệ thống mạng.

Các phương pháp kiểm tra hành động sẽ dựa vào nội dung của traffic để đưa ra kết luận traffic đó có chứa mã độc hay không.

Phương pháp phân tích, kiểm tra cũng góp phần không nhỏ cho việc phát hiện và xác định các dạng tấn công chưa được cập nhật trong cơ sở dữ liệu Signature-based, giúp cơ sở dữ liệu ngày càng đầy đủ, đa dạng hơn.

3.2.3.1 Pattern Detection

Pattern Detection là phương thức kiểm tra đơn giản nhất, cơ chế hoạt động theo phương thức so trùng. Trước hết cần phải định nghĩa ra một dấu hiệu (một chuỗi text, hình ảnh, dữ liệu…) trong Signatured-based để khi phân tích, dấu hiệu này sẽ là mẫu để

để kiểm tra các traffic. Khi IPS phát hiện nội dung của traffic có chứa những đoạn mã giống với mẫu thì IPS sẽ đưa hành động đáp trả hợp lý.

Ngoài ra IPS còn có khả năng xử lý với những kiểu dữ liệu được hoán vị khác, có nội dung khác so với mẫu.

Pattern Detection có thể kết hợp với Atomic signature và Stateful signature.

❖ Ưu điểm

Là phương pháp ngăn chặn mạnh mẽ nếu có một Signature-based phong phú và được cập nhật liên tục, có những dấu hiệu rõ ràng cho mỗi lần thực hiện hành động đáp trả, giúp nhà quản trị dễ dàng nhận thấy và khắc phục.

❖ Nhược điểm

Vì cơ chế hoạt động quá đơn giản, nên việc linh hoạt trong một hệ thống mạng với nhiều loại traffic, tỉ lệ mà Pattern Detection sẽ tạo ra những hành động mang tính False Positive rất cao, đặc biệt nếu được áp dụng với Atomic Signature. Đồng thời, thời gian kiểm tra các traffic sẽ dài.

3.2.3.2 Signature-based Detection

Phương pháp kiểm tra này là một dạng của phương pháp Pattern Detection, dựa vào cơ sở dữ liệu có sẵn bao gồm Exploit-based signatures và Vulnerability-based signatures. Exploit-based signatures sẽ đưa ra thông tin về các dấu hiệu bất thường gây ảnh hưởng trực tiếp tới hệ thống endpoint, còn Vulnerability-based phân tích phát hiện lỗ hổng bảo mật của một hệ thống hoặc một chương trình, từ đó IPS sẽ dựa vào cơ sở dữ liệu này để thực hiện việc kiểm tra hệ thống.

❖ Ưu điểm

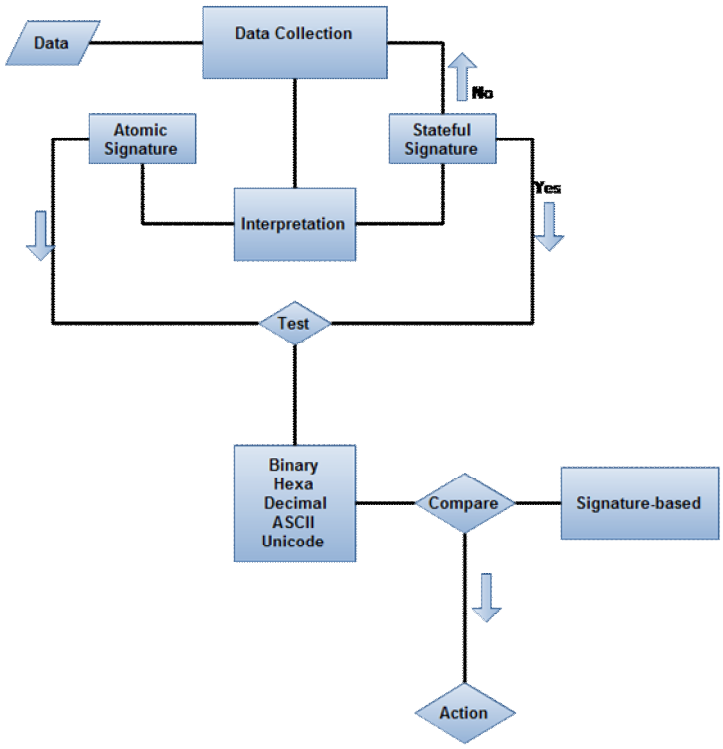
Đơn giản, dễ sử dụng, ít bỏ sót khi phát hiện ra các traffic có dấu hiệu bất hợp pháp khi tìm thấy thông tin về các dấu hiệu này trong cơ sở dữ liệu. Linh hoạt trong việc thay đổi tùy chỉnh lại cơ sở dữ liệu để thích hợp với hệ thống của mình.

❖ Nhược điểm

Không thể phát hiện ra những biến thể hoặc các phương thức tấn công khác ngoài cơ sở dữ liệu sẵn có. Ví dụ đơn giản chính là sự thay đổi cách tấn công của các biến thể worm.

Do sử dụng những dấu hiệu nên các đối tượng tấn công sẽ dễ dàng biết được và thay đổi phương thức tấn công. Đặc biệt ban đầu, dễ dàng nhầm lẫn khi các hành động này không nằm trong cơ sở dữ liệu. Có thể tạo ra những hành động mang tính False Positive cao. Có thể chỉnh sửa trong cơ sở dữ liệu để hạn chế tình trạng này.

Đảm bảo Signature-based được cập nhật thường xuyên.



Hình B1 – 1 : Signature-Based Detection

3.2.3.3 Statistical Profile-based Detection

Statistical Profile-based Detection (hay còn gọi là Profile-based Detection), quá trình kiểm tra của Profile-based Detection không dựa vào một hành động rõ ràng nào (khác với Pattern Detection là đòi hỏi một dấu hiệu rõ ràng), phương thức này sẽ đưa ra hành động đáp trả hợp lý khi phát hiện một hành động bất thường nào đó xảy ra.

Statistical Profile-based Detection sẽ tạo ra một Profile-based signature chứa các định nghĩa về lưu lượng và dạng traffic thường có trong một môi trường hoạt động tại một thời điểm được xem là hệ thống hoạt động bình thường, đúng tiêu chuẩn (thường được tạo ra khi hệ thống mạng vừa được xây dựng hoàn chỉnh).

Trong suốt quá trình theo dõi hệ thống, nếu IPS phát hiện bất kỳ đối tượng nào có dấu hiệu vượt quá những định nghĩa về tiêu chuẩn được đề ra trong Profile-based Signature, thì xem như đối đượng đó là bất thường, khi đó IPS sẽ đưa ra những thông tin cảnh cáo và những hành động thích hợp.

❖ Ưu điểm

Nhanh chóng phát hiện để xử lý kịp thời, có khả năng phát hiện những hành động tấn công mới xuất hiện, chưa phát tán rộng rãi. Không cần phải định nghĩa một lượng lớn signatures, khả năng phát hiện được những bất thường xảy ra trong hệ thống mạng rất cao khi kết hợp với Signature-based.

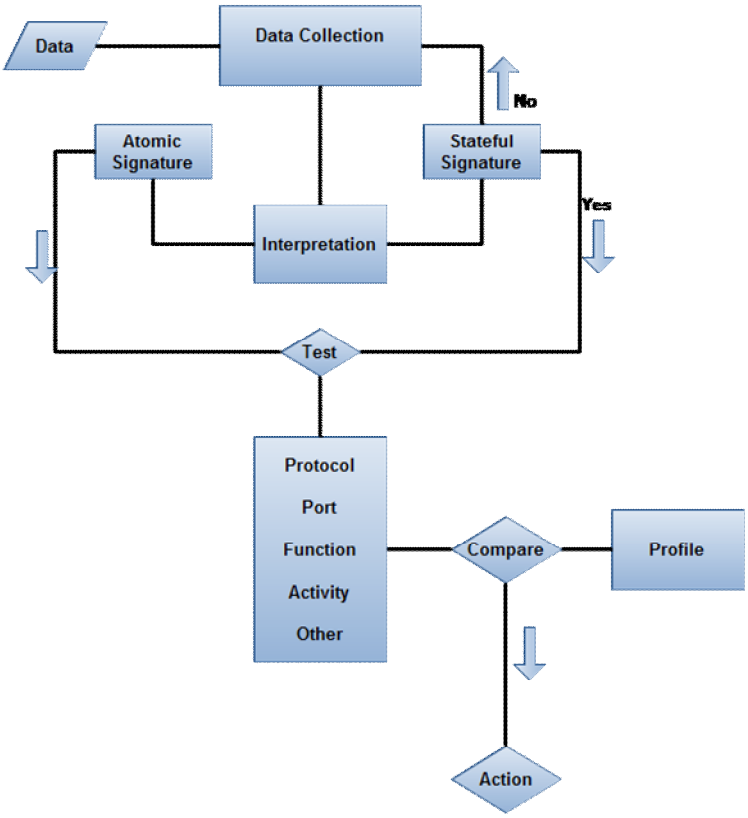
Các đối tượng tấn công thường đi tìm những nguyên nhân dẫn đến sự ngăn cản và cảnh báo của hệ thống IPS rồi từ đó tìm hướng tấn công khác, tuy nhiên, với Profile-based Detection này thì attacker không thể biết được IPS dựa vào cơ sở gì để phát hiện ra sự tấn công của họ, làm cho độ an toàn hệ thống được cao hơn.

❖ Nhược điểm

Đòi hỏi sự hiểu biết nhiều về hệ thống, và sẽ gặp khó khăn trong các hệ thống mạng có quy mô lớn (là một mô hình hỗn hợp gồm nhiều hệ thống khác nhau, nhiều thiết bị, tập hợp nhiều chương trình ứng dụng), đòi hỏi nhu cầu, yêu cầu cao và thay đổi thường xuyên.

Không linh hoạt, gây khó khăn khi có nhu cầu thay đổi về hệ thống. Đôi khi gây ra những thông báo không chính xác về sự thay đổi của hệ thống, sự tấn công.

Profile-based do phải dùng một dạng tiêu chuẩn chung, mang tính tổng thể nên thể hiện sự không chính xác, không rõ ràng, bên cạnh đó, các cảnh báo không thể hiện đầy đủ chi tiết các thông tin cho việc phân tích và gây trở ngại cho việc phân tích, khắc phục, và phát triển hệ thống. Đồng thời khi có sự thay đổi trong hệ thống thì phải tạo ra một Profile-based mới.



Hình B1 – 2 : Profile-Based Detection

3.2.3.4 Behavior-based Detection

Behavior-based Detection : Phương thức này gần giống phương thức Pattern Detection, tuy nhiên Behavior-based không sử dụng dấu hiệu rõ ràng, mà dựa vào các hoạt động được cho là đáng ngờ dựa và việc phân tích các hành động ở từ thời điểm đó trở về trước.

Behavior-based Signatures là tập hợp những class, mà trong những class này định nghĩa những hoạt động được cho là đáng ngờ. IPS sẽ tạo ra một hệ thống ảo, và sẽ chạy thử dữ liệu thu thập được, dựa vào những hành động này, IPS sẽ tiến hành đánh giá và

đưa ra quyết định đó có phải là hoạt động bất thường hay không để đưa ra hành động đáp trả hợp lý.

Bên cạnh đó, phương thức này còn hỗ trợ việc sử dụng một Signature để định nghĩa chung cho tất cả các hoạt động có cơ chế tương tự mà không cần phải định nghĩa riêng cho từng hành động. Ví dụ khi phát hiện một ứng dụng lợi dụng giao thức e-mail để thực thi những lệnh CLI, với cơ chế Behavior-based Detection, tự động IPS sẽ đưa ra hành động ngăn chặn tất cả các ứng dụng liên quan tới giao thức e-mail ở host.

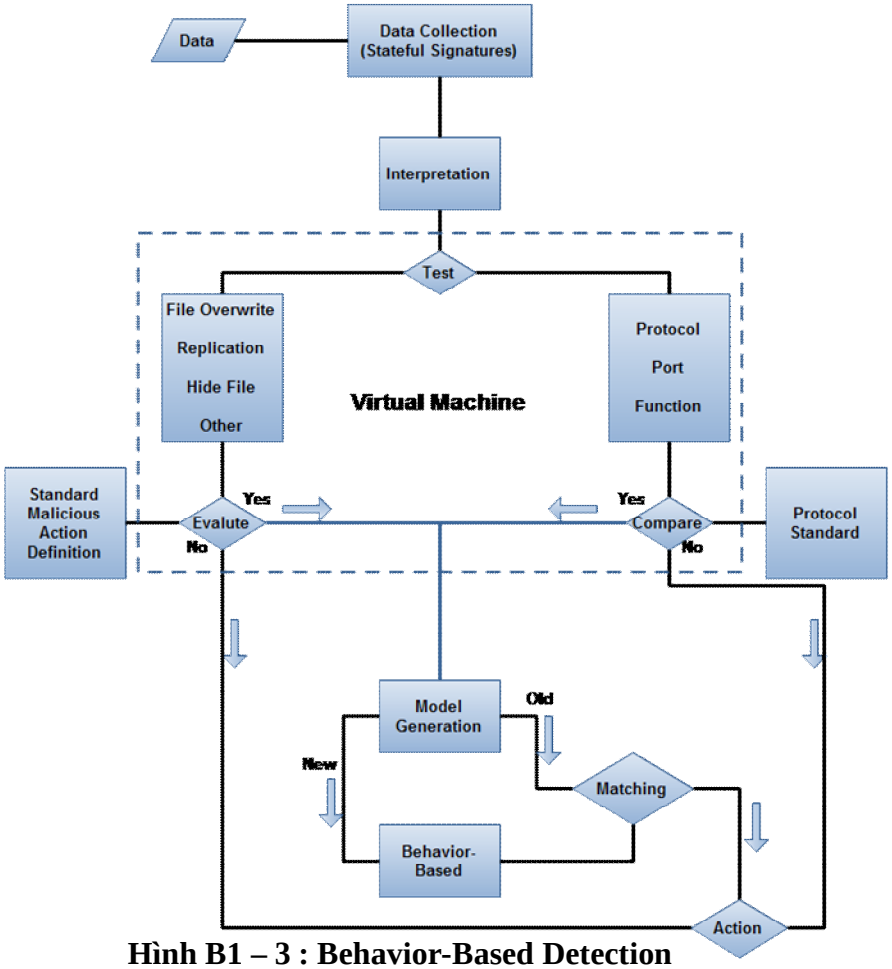
❖ Ưu điểm

Do các hành động bất thường đều được định nghĩa dựa theo một tiêu chuẩn nào đó do nhà cung cấp dịch vụ (Avira, Kaspersky…) đưa ra, hạn chế được số lượng Signature-based. Với phương pháp này, IPS dễ dàng phát hiện ra các hoạt động bất thường, và nếu những hoạt động này chưa được trong cơ sở dữ liệu thì IPS sẽ tự động cập nhật để tiện cho việc kiểm tra lần sau.

❖ Nhược điểm

Đôi khi dẫn đến gây ra các hành động đáp trả mang tính False Positve.

Không định nghĩa chi tiết dạng tấn công, do đó việc thông tin cảnh báo và log không đầy đủ chi tiết, dẫn đến khó khăn trong việc phát hiện, và khắc phục.



Hình B1 – 3 : Behavior-Based Detection

3.2.4 Signature Action

3.2.4.1 Generating and alert

Có hai dạng thông báo là Atomic alerts và Sumary alerts

- Atomic alerts

Mỗi khi phát hiện hoạt động bất hợp pháp, IPS sẽ tạo ra một cảnh báo tới quản trị viên về hoạt động đáng ngờ bị phát hiện. Tuy nhiên, phương thức tạo cảnh báo này dễ bị attacker khai thác, attacker sẽ tạo ra một loạt các hành động vi phạm để IPS cảnh báo liên tục, dẫn đến hệ thống log quá tải và quản trị viên tràn ngập trong các cảnh báo.

- Sumary alerts

Tất cả những cảnh báo về các hoạt động có cùng kiểu vi phạm, cùng những thông tin (Source IP, destination IP, port…) sẽ được đưa chung lại vào một gói tin cảnh báo duy nhất, tuy nhiên vẫn thể hiện đầy đủ thông tin như số lần vi phạm, thời gian, kiểu vi phạm. Trong suốt thời gian bị tấn công, mỗi Signature đều có một được định nghĩa một khoảng interval, nếu các hành động vi phạm kéo dài thì khi thời gian interval hết thì cảnh báo mới sẽ được gửi đi. Với phương pháp này đã khắc phục được điểm yếu của phương thức Atomic alerts.

3.2.4.2 Drop Signature Action

Khi phát hiện traffic vi phạm, IPS có nhiều cách thức để hạn chế sự vi phạm đó, việc ngăn chặn và loại bỏ gói tin nếu cần thiết. Với hành động drop gói tin của IPS giúp cho hệ thống bảo vệ chặn đứng được mối nguy hiểm từ các hoạt động tấn công. Tuy nhiên, với phương thức này, attacker vẫn có thể tiếp tục tấn công vào hệ thống với các gói tin khác.

3.2.4.3 Log Signature Action

Đôi khi phát hiện những hành động bất thường, tuy nhiên do không đủ thông tin hoặc cơ sở cho rằng đó là một hành động vi phạm, ta có thể lưu lại vào log và cho những traffic này đi qua. Tuy nhiên dựa vào log ta sẽ theo dõi, đánh giá và đưa ra những hành động phù hợp sau đó.

3.2.4.4 Block Signature Action

Khi dùng Block Signature Action, nếu IPS phát hiện các gói tin vi phạm liên tiếp từ một nguồn thì IPS sẽ tạo ra một Access Control List (ACL) để chặn tất cả các traffic khởi tạo từ phía attacker mà không cần trải qua các chu trình kiểm tra phức tạp.

3.2.4.5 TCP Reset Signature Action

Khi phát hiện traffic vi phạm thì IPS sẽ gửi gói tin chứa cờ RST cho cả hai endpoint để yêu cầu tạo kết nối mới.

3.2.4.6 Allow Signature Action

Traffic không thuộc bất cứ dạng nào nằm trong danh sách ngăn chặn của IPS thì sẽ được cho phép đi tiếp thông qua Outbound Interface của IPS.

B . Checkpoint Solutions

1 Checkpoint IPS Protection

Hệ thống bảo vệ của IPS tập trung vào ba phần chính

1.1 Network Security

- Bảo vệ hệ thống trước những cách thức tấn công dựa vào việc thay đổi nội dung các trường trong những gói tin TCP, như Sequence number, Checksum…
- Xây dựng hệ thống quản lý các kết nối hạn chế tình trạng overload tài nguyên của hệ thống IPS nhằm tối ưu tính hiệu năng của hệ thống.
- Bảo vệ hệ thống trước những phương thức tấn công DoS, Buffer Overflow.
- Bảo vệ hệ thông mạng trước những phương thức Reconnaissance để lấy thông tin về hệ thống như sơ đồ mạng, các hệ điều hành được sử dụng trong hệ thống mạng…
- Cung cấp danh sách những địa chỉ IP được cho là thường được sử dụng để tấn công vào hệ thống, giúp các nhà quản trị viên có thể thiết lập Rule ngăn chặn các traffic từ những địa chỉ này.
- Bảo vệ hệ thống trước những phương thức tấn công ở lớp Transport thông qua giao thức TCP.

1.2 Application Intelligent

- Hỗ trợ xây dựng chính sách giới hạn và yêu cầu về tính chính xác của phương thức được sử dụng trong các giao thức POP3, SMTP, FTP, TELNET… trước những phương thức tấn công Malformed command hay Buffer Overflow…
- Xây dựng hệ thống quản lý các ứng dụng Instanct Message như Yahoo Messenger, Skype… quản lý các chương trình sử dụng giao thức Peer-to-Peer.
- Khắc phục những lỗ hổng bảo mật của một số ứng dụng có thể bị khai thác (IAS, Adobe products, Outlook…) bằng Buffer Overflow, hoặc Malformed Packet…
- Hỗ trợ giao thức VPN, loại bỏ những gói tin IKE được chỉnh sửa nhằm gây DoS hệ thống trong các giao thức SSL VPN. Chỉ định phương thức IKE chỉ được sử dụng trong quá trình xây dựng VPN Tunnel, IPS sẽ loại bỏ những quá trình đàm phán IKE sử dụng Aggressive Mode…
- Bên cạnh đó IPS còn hỗ trợ nhiều giao thức và các ứng dụng khác như DNS, IBM database, Oracle Database…

1.3 Web Intelligent

- Xây dựng hệ thống bảo vệ hệ thống Web Server trước những phương thức tấn công DoS như Buffer overflow.
- Xây dựng hệ thống bảo vệ hệ thống Web Server trước những phương thức tấn công bằng mã độc, lỗ hổng khi xây dựng cơ sở dữ liệu (SQL, LDAP).

- Bảo vệ hệ thống endpoint Client trước những tấn công lợi dụng lỗ hổng của trình duyệt như Internet Explorer va các addon được cài đặt ở các trình duyệt như Adobe Flash… nhằm gây Buffer overflow và chiếm quyền hệ thống.

2 IPS Optimization

2.1 Trouble Shooting

Khi thiết lập một hệ thống IPS, việc enable chức năng Trouble Shooting sẽ rất hiệu quả cho việc đánh giá hiệu suất hoạt động của IPS đối với các hoạt động mạng, với cơ chế Detect-Only, IPS sẽ kiểm tra, phân tích và tạo ra những file log về các hoạt động, traffic trong hệ thống mạng, nhờ đó, ta có thể dễ dàng đánh giá mức độ hoàn thiện của IPS.

2.2 Protect Internal Host Only

Đối với một IPS được tích hợp sẵn trên Gateway, hoặc được thiết kế trên một thiết bị riêng thì vấn đề hiệu suất hoạt động của IPS luôn là vấn đề cần quan tâm. Đối với hệ thống tích hợp IPS, việc sử dụng chung một tài nguyên, hệ thống thì sự ảnh hưởng lẫn nhau cần được quan tâm.

Nếu IPS tham gia, thực hiện quá nhiều chu trình giám sát kiểm tra, xử lý các traffic trên mạng, thì hiển nhiên lượng tài nguyên hệ thống của IPS phải chiếm nhiều, đồng thời có thể ảnh hưởng đến hiệu năng của hệ thống mạng. Do đó, để giới hạn sự tham gia của IPS, ta có thể hạn chế quá trình phân tích, kiểm tra bằng cách chỉ bảo vệ mạng Private.

2.3 Bypass Under Load

Bằng phương pháp này, IPS sẽ được tắt (inactive) trong một khoảng thời gian khi hệ thống trở nên chậm chạp vì một lý do gì đó. Khi đó IPS sẽ không tham gia quá trình kiểm tra, phân tích các traffic, nhằm tránh gây ra hiện tượng overload hệ thống, dẫn đến hệ thống bị tắt nghẽn.

Việc inactive chức năng IPS trong một thời gian ngắn cũng không ảnh hưởng nhiều đến hệ thống bảo mật, vì hệ thống Firewall một phần đã có khả năng ngăn chặn được các hiểm họa. Chỉ vì khi bật IPS được tích hợp lên, các dữ liệu đầu tiên sẽ được Firewall của hệ thống kiểm tra và sau đó gửi tới IPS để tiếp tục thực hiện quá trình phân tích, tắt IPS chỉ đơn giản giảm bớt một hệ thống bảo mật, và không ảnh hưởng nhiều tới hệ thống. Và sau một khoảng thời gian, khi khả năng xử lý của hệ thống trở lại một mức nào đó được ta định sẵn thì IPS tự động được kích hoạt.

Trong thời gian IPS inactive, ta vẫn có thể kiểm tra hoạt động của traffic trong hệ thống mạng, bao gồm log, mail alert, popup alert, SNMP Trap alert.

Với mode “Advanced”, ta có thể điều chỉnh các thông số định nghĩa “Heavy Load” để IPS có thể tự động tắt, mở giúp hệ thống được tối ưu hơn.

- High : Nếu hệ thống tài nguyên CPU và Memory của hệ thống vượt ngưỡng này thì IPS sẽ tự động được tắt để tăng hiệu suất làm việc cho hệ thống.
- Low : Nếu IPS ở trạng thái tắt, khi tài nguyên hệ thống CPU và Memory đạt ngưỡng Low trở xuống thì IPS sẽ tự động được bật lên.

CHAPTER 03 – EPS ENDPOINT SECURITY (SECURE ACCESS)

Trong chapter này ta sẽ nói về Endpoint Security và các vấn đề về quá trình cấu hình, quản lý và cấp Policy cho End-point Users.

Ngoài ra còn có phần Cooperative Enforcement giúp quản lý End-point Users được chặt chẽ thông qua quá trình kết hợp làm việc của các thiết bị mạng đảm nhận các vị trí khác nhau.

Chapter 03 – Endpoint Security bao gồm bốn phần

- *EPS Overview*
- *Managing Catalogs*
- *Managing Security Policy*
- *Gateway and Cooperative Enforcement*

❖ EPS Overview

Trong phần EPS Overview ta sẽ giới thiệu tổng quan về cấu trúc, Policy, các chế độ hoạt động, quản lý Domains, quản lý vai trò của Administrator trong EPS Server.

- EPS System Architecture
- Policy Overview
- Modes and Views
- Managing Domain
- Managing Administrator Role

❖ Managing Catalogs

Trong phần này ta sẽ giới thiệu về các phương thức quản lý Endpoint Clients thông qua Username và IP Adress.

Ngoài ra còn các vấn đề liên quan tới quá trình xác thực khi sử dụng User Catalogs.

- User Catalogs
- IP Catalogs

❖ Managing Security Policy

- Policy Types
- Creating Policy
- Policy Object

❖ Gateway and Cooperative Enforcement

- Cooperative Enforcement Overview
- Network Access Server Integration
  - Cooperative Enforcement – NAS Architecture
  - Cooperative Enforcement – NAS Workflow

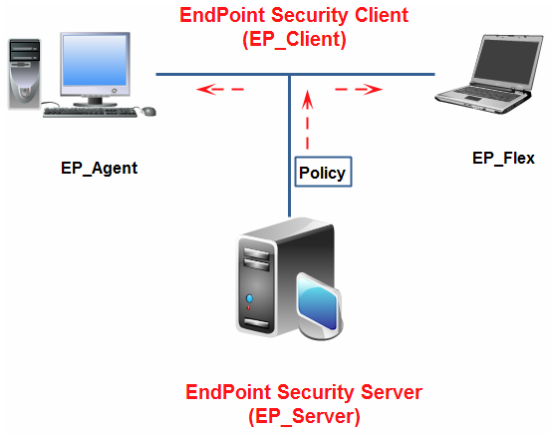
A . EPS Overview

Endpoint Security cho phép quản trị viên quản lý tập trung tất cả các hệ thống máy end-point khi tham gia vào hệ thống mạng do chúng ta quản lý thông qua policy, bao gồm triển khai, giám sát và quy định những chính sách bảo mật đối với các hệ thống máy end-point.

1 EPS System Architecture

Hệ thống Endpoint Security có 2 phần cơ bản : Endpoint Security Server (EP_Server) và Endpoint Security Client (EP_Client). Bên cạnh còn có Security Gateways, RADIUS servers, LDAP servers…

- EP_Server là thiết bị thiết lập và triển khai các Enterprise Policies.



Hình C1 – 1 : EPS System Architecture

- EP_Client package là phần mềm được cài trên máy end-point. EP_Client sẽ thường xuyên cập nhật đồng bộ thông tin với EP_Server để cập nhật các Enterprise Policies từ EP_Server, giám sát và thực thi các Enterprise Policies nhận được từ EP_Server. Có bốn dạng Endpoint Security Client

  - EP_Agent

    EP_Agent có giao diện đơn giản, được sử dụng đối với các hệ thống máy luôn thường trực trong mạng được quản lý (Desktop PC) tuy nhiên vẫn có thể sử dụng với các Remote Users hoặc thiết bị di động (Laptop. Bao gồm giao diện đơn giản, không cho phép các Users tiến hành chỉnh sửa hoặc thay đổi thông tin bảo mật được cấu hình sẵn từ Admin.

  - EP_Flex

    Sử dụng EP_Flex cung cấp cho Users nhiều quyền hơn trong việc quản lý thiết lập các chính sách riêng cho mình (Personal Policy). EP_Flex phù hợp dùng cho những Remote Users, các thiết bị di động (Laptop).

  - VPN Agent và VPN Flex

    Bên cạnh những chức năng thông thường như bảo vệ hệ thống, dữ liệu, Endpoint Security cung cấp chức năng quản lý quá trình truy xuất của các Remote Users thông qua VPN.

2 Policy

2.1 Policy Overview

Policy là chính sách bảo mật được nhà quản trị (Admin) triển khai và áp đặt đến từng Users trong hệ thống mạng của mình bằng cách tạo ra những Enterprise Policies và chỉ định những policies này đến từng User hoặc nhóm các Users (User Groups) thông qua một chương trình giao tiếp giữa EP_Server và EP_Users (được cài đặt ở hệ thống máy của Users, được gọi là EP_Client package). Và những policies này sẽ được thực thi bởi EP_Client package ở các hệ thống của Users. Đối với Users sử dụng EP_Flex package thì Users có thể tự định nghĩa Personal policy.

Các vấn đề của Policy sẽ được đề cập chi tiết trong phần C "Managing Policy Server".

2.2 Policy Component Overview

❖ Firewall Rules

Hoạt động như một Firewall truyền thống, bao gồm kiểm tra các thông tin IP, port source và port destination (block hoặc allow traffic thông qua việc kiểm tra các gói tin communication) và cả thời gian cho từng Rule. Hoạt động chủ yếu ở lớp Network.

❖ Zone Rules

Quản lý những luồn traffic đến và khởi tạo từ các Zone do quản trị viên định nghĩa trước. Bao gồm Blocked Zone, Internet Zoned, Trusted Zone.

❖ Program Control

Sử dụng cơ chế Program Advisor hạn chế quá trình truy xuất trao đổi thông tin qua mạng của các chương trình. Program Control cho phép hạn chế thiết lập quản lý quá trình truyền thông của một chương trình cụ thể giữa Trusted Zone và Internet Zone.

❖ Program Advisor

Checkpoint sẽ hỗ trợ EP_Server và EP_Users về các chính sách dành cho từng chương trình có chức năng mạng, nhằm tiết kiệm thời gian và giảm bớt lượng công việc cho nhà quản trị.

❖ Enforcement Rules

Nhằm đảm bảo chính sách bảo mật của hệ thống mạng luôn được thực hiện chính xác, Enforcement Rules sẽ thực thi những yêu cầu đòi hỏi về tiêu chuẩn bảo mật (do admin đề ra) của hệ thống EP_Users khi tham gia vào hệ thống mạng được quản lý. Nếu hệ thống EP_Users không đáp ứng được những yêu cầu này, thì kết nối của hệ thống EP_Users sẽ bị hạn chế sự kết nối vào mạng.

❖ Anti-Spyware

Bảo vệ EP_Users và hệ thống mạng trước những nguy hiểm từ Worm, Trojan…

❖ Anti-Virus

Bảo vệ EP_Users trước những loại Virus đã biết và phòng ngừa những loại Virus chưa xuất hiện.

❖ SmartDefence

Bảo vệ hệ thống mạng trước những cuộc tấn công Network Attack như DoS. Ngăn chặn những phương thức tấn công dạng che giấu (Over channel : sử dụng những giao thức bất hợp pháp thông qua giao thức hợp pháp trong hệ thống mạng …) hoặc các dạng tấn công vào tiêu chuẩn (RFC) để tạo ra các malform packet làm ảnh hưởng đến hệ thống.

❖ Mail Protection

Ngăn chặn các cuộc tấn công bằng mail (Mailsafe), giới hạn số lượng mail được gửi đi nhằm hạn chế các loại worm lợi dụng Mail và EP_Users để lây lan sang các hệ thống khác trong mạng.

3 Modes and Views

3.1 Multi-Domain Mode

Ở Multi-Domain Mode, ta có thể tạo ra nhiều domain nhỏ hơn, dễ dàng cho việc quản lý các Users và áp đặt các policies cho từng User cụ thể. Mỗi domain có thể có riêng một quản trị viên riêng để quản lý domain đó, bao gồm quản lý User (chia group) và xây dựng policy riêng cho từng User và User Group trong domain đó.

3.2 Single Domain Mode

Single Domain Mode : Việc sử dụng Single Domain ít linh hoạt hơn Multi-Domain tuy nhiên có thể quản lý user theo dạng group và áp đặt policy cho từng group.

Đối với Single Domain Mode, sẽ có 2 giao diện sử dụng

- ❖ Simple View : Giao diện đơn giản hỗ trợ giám sát, tạo và áp đặt policy.
- ❖ Advanced View : Giao diện hỗ trợ sử dụng tất cả các tính năng mà Simple View không hỗ trợ (Domain và Catalogs, Policy Template, Policy Assignment…).

4 Managing Domain

4.1 Multi-Domain Administrators

Global Administrator : Là Admin có quyền truy xuất và quản lý tất cả các domain, bao gồm tạo, quản lý domain, policy (cho tất cả các domain).

Domain Administrator : Mỗi Domain được tạo ra và được quản lý bởi một quản trị viên có quyền tạo và chỉ định policy cho từng User/Group. Giám sát và xử lý các vấn đề về kết nối giữa các Endpoint, và các báo cáo về hoạt động của các Users trong domain mình quản lý.

4.2 System Domain và Non-System Domain

4.2.1 System Domain

Cung cấp chức năng quản lý tập trung các domain. Tạo các policy ảnh hưởng tới tất cả các Non-System Domain. Chỉ có Global Administrator mới có quyền truy xuất vào

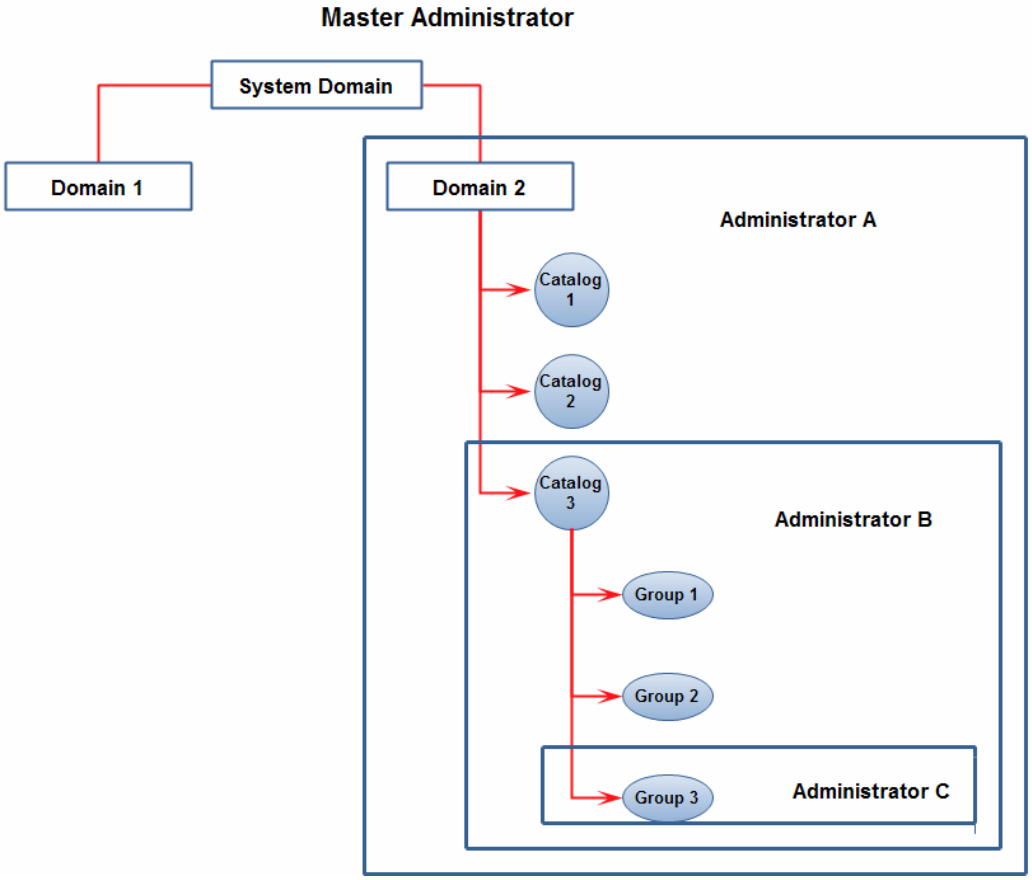
System Domain. Những thay đổi của System Domain mang tính Global ảnh hưởng tới tất cả các non-System Domain.

4.2.2 Non-System Domain

Là những domain được tạo bởi System Domain, chỉ có thể quản lý những EP_Users thuộc domain đó.

5 Managing Administrator Roles

Administrator chỉ có thể chỉ định policies từng User hoặc Group thuộc domain mà Admin đó quản lý.



Hình C1 – 2 : Administrator Role Example

- Domain Manager : Tạo, chỉnh sửa, xóa thông tin và domain của Endpoint Security (trong system domain).
- Entity Manager : Tạo, chỉnh sửa, xóa nội dung thông tin của Endpoint Security (non-system domain).
- Admin Manager : Tạo, thay đổi và xóa các quyền của Administrator domain.
- Even Notification : Thông báo cho Admin về những hoạt động của hệ thống và tạo những tập tin log về các hoạt động (System Domain).
- Program Advisor : Điều chỉnh những thiết lập của Program Advisor.

- Assignment Priority : Chỉ định policy gán cho các EP_Users khi có nhiều policy gán cho User này, hoặc do User này thuộc nhiều Catalog (sẽ đề cập ở phần Managing Catalog) (System Domain).
- Certificate : Tạo và xóa Certificate.
- Client Package : Tạo những gói EP_Client package để triển khai đến các EP_Users.
- Firewall Rule Management : Tạo, xóa và chỉnh sửa những rule của Firewall của các policy.
- Enforcement Rule Manager : Tạo, xóa và chỉnh sửa các Enforcement Rule của các policy.
- Template Publishing : Tạo, chỉnh sửa những kiểu mẫu (policy) và áp dụng cho tất cả các domain (System Domain).
- Policy Assignment : Chỉ định policy cho domain hoặc đối tượng.
- Policy Deployment : Triển khai policy trên policy server.
- Reports : Bật chức năng báo cáo.

B . Managing Catalogs

Endpoint Security hỗ trợ hai loại Catalog cho việc quản lý Users

- *User Catalogs : Dựa vào những cơ sở dữ liệu về các tài khoản của Users của hãng thứ ba (Third Party) như : LDAP, NTDomain, RADIUS. Bên cạnh đó, Endpoint Security còn có thể xây dựng cơ sở dữ liệu nội bộ của chính Endpoint Security như Custom Catalogs, Custom Groups.*
- *IP Catalogs : Quản lý Users dựa vào địa chỉ IP và Subnet Mask.*

1 User Catalogs

Sử dụng User Catalogs để chỉ định policy dựa vào nhiệm vụ, vị trí và trách nhiệm của EP_Users trong một bộ phận của công ty. Ví dụ như EP_Users Manager của bộ phận Marketing có quyền truy xuất thông tin của các thành viên trong bộ phận đó, và các thành viên trong bộ phận đó lại không được truy xuất thông tin của nhau hoặc của Users quản lý. Admin có thể áp đặt policies khác nhau, tùy thuộc vào vị trí, trách nhiệm của từng Users.

Nếu một User thuộc nhiều Catalog và group, và sẽ nhận được nhiều policy từ các Catalog và group đó, thì EP_User sẽ thực thi thực thi policy nhận được đầu tiên.

1.1 Custom Catalogs

Trong Custom Catalogs ta có thể linh hoạt cấp policy cho từng User thông qua phương pháp tạo nhiều group trong Custom Catalog.

Ở mỗi trường UserID (khi tạo EP_Client Package) ta ghi rõ đường dẫn theo cú pháp

manual://<Catalog type>/<group>

Khi admin gán policy cho group hoặc cả Catalog thì tất cả những EP_Users cài đặt EP_Client package đó sẽ bị ảnh hưởng mà không cần kiểm tra Users hoặc IP.

1.2 LDAP Catalogs

Endpoint Security cung cấp những thông tin cấu hình sẵn với Novel eDirectory (Novel), Netscape Directory Server (Windows 2000), Windows Active Directory (AD). Hoặc nếu có sử dụng một LDAP Server khác như ADAM thì Admin phải tự cấu hình các thông số cần thiết ở các trường trong quá trình tạo LDAP Catalog (Catalog Information) để LDAP Server đó có thể trao đổi đồng bộ thông tin với Endpoint Security.

Dựa vào những thuộc tính User Attribute của mỗi hệ thống LDAP, EP_Server sẽ tiến hành giao tiếp trao đổi thông tin của User đó. Quá trình xác thực User dựa vào hai phương thức là EP_Users sẽ xác thực với LDAP bằng cách *Join Domain* (Microsoft Active Directory) hoặc EP_Server sẽ đóng vai là một RADIUS Proxy Server thông qua sử dụng chức năng "Proxy Login Server" nếu EP_Users không *Join Domain*.

Chức năng "Auto add" giúp những Users khi xác thực thành công mà chưa được cập nhật trong cơ sở dữ liệu của hệ thống EP_Server thì lập tức được cập nhật vào EP_Server.

- Proxy Login Server

Endpoint Security đóng vai RADIUS Proxy Server, tiếp nhận những yêu cầu xác thực và tiến hành gửi yêu cầu xác thực đến LDAP Server. Đối với phương thức

này, do EP_Server chỉ hỗ trợ phương thức xác thực Simple Authentication khi trao đổi với LDAP Server, vì thế traffic giữa EP_Server và LDAP Server hoàn toàn là cleartext.

❖ Join Domain

Trước tiên, EP_User sẽ xác thực với LDAP server qua bước Log On, sau đó sẽ tiến hành trao đổi thông tin với EP_Server (thông tin đã được mã hóa). Nếu EP_User được xác thực thành công EP_Server sẽ cấp đúng policy cho từng User (nếu User đó đã được cập nhật trong cơ sở dữ liệu của EP_Server) hoặc sẽ cấp policy chung cho của Catalog (nếu user đó chưa được cập nhật trong database của EP_Server).

1.3 RADIUS Catalogs

Một RADIUS Server có thể bao gồm Internal (TACACS+) và external User database (LDAP), tiếp nhận những yêu cầu xác thực từ EP_Server (EP_Server đóng vai RADIUS Proxy Server), và RADIUS Server sẽ tiến hành xác thực những thông tin đó, trả kết quả về cho EP_Server. RADIUS Catalog hỗ trợ phương thức mã hóa trong quá trình trao đổi thông tin xác thực giữa EP_Server và RADIUS Server, giúp thông tin xác thực của EP_Users được an toàn hơn so với hệ thống xác thực giữa EP_Server và LDAP Server.

1.4 Synchronizing User Catalogs

Đồng bộ thông tin giúp EP_Server cập nhật những thông tin mới về EP_Users ở các hệ thống LDAP hoặc NT Domain, ta có thể thực hiện quá trình đồng bộ theo một lịch định sẵn hoặc đồng bộ thủ công.

Các thông tin được đồng bộ

- Những cập nhật mới vừa được đưa vào EP_Security, những Users mới sẽ nhận những policy của group hoặc catalog chứa chúng.
- Những thông tin vừa bị xóa khỏi Endpoint Security, các EP_Users nhận được những policy đó vẫn áp dụng chúng bình thường, không thay đổi cho tới khi lần trao đổi thông tin giữ EP_Server và EP_Users xảy ra (phụ thuộc vào HeartBeat).
- Những group sau khi cập nhật được thay đổi tên xem như group cũ là đã bị xóa khỏi Endpoint Security và group mới được cập nhật. Trong trường hợp này, policy chỉ định cho group cũ xem như không còn ảnh hưởng tới các Users trong group đó, phải chỉ định policy cho group mới.

1.5 Authenticating Users

Endpoint Security sẽ đóng vai như một Proxy Login Server, tiến hành gửi yêu cầu xác thực EP_Users đến các Authentication Server.

❖ Gateway Authentication

Users kết nối vào mạng được quản lý thông qua một gateway. EP_Server sẽ chỉ định policy định sẵn vào gateway và tất cả các EP_Users truy xuất vào hệ thống mạng thông qua Gateway này sẽ nhận policy được áp đặt cho chính Gateway này.

❖ Native Authentication

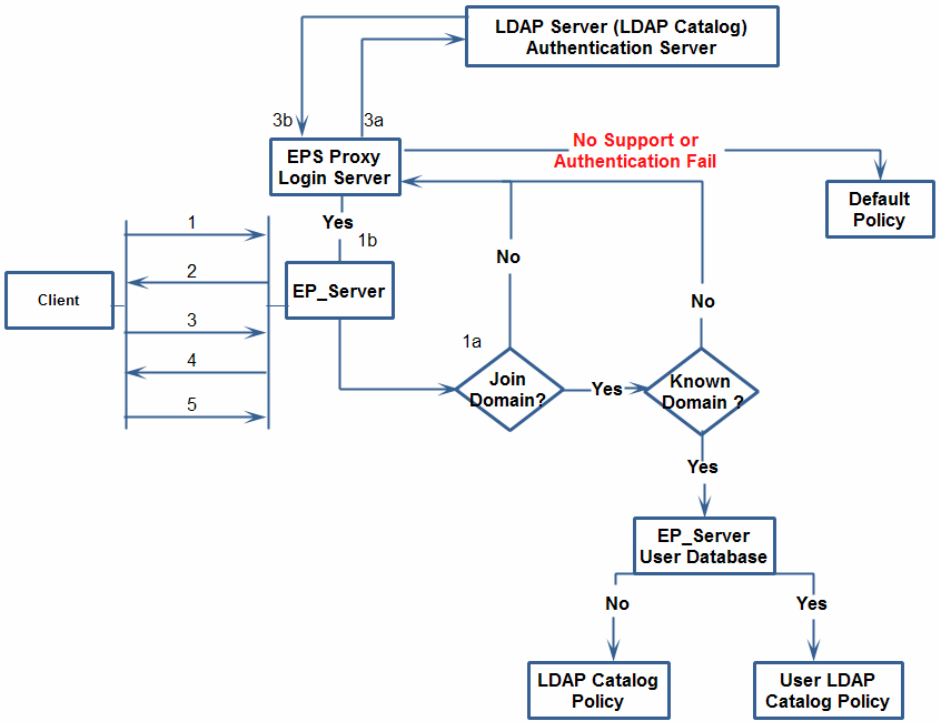
Nếu sử dụng quá trình xác thực bằng hệ thống NT Domain, Novell NDS LDAP, Microsoft Active Directory, các EP_Users sẽ xác thực với LDAP Server sau đó Endpoint Security sẽ tự động chỉ định các EP_Users thông qua những thông số EP_User gửi tới.

❖ Proxy Login Server

Nếu sử dụng hệ thống xác thực RADIUS hoặc LDAP (ngoài hệ thống Novell NDS và Microsoft Active Directory do xác thực dạng Native), EP_Server đóng vai là RADIUS Proxy server.

1.6 Authentication Process

1.6.1 LDAP Catalog



Hình C2 – 1 : LDAP Catalog Authentication Process.

Bước 1 : EP_User khởi tạo kết nối đến EP_Server cung cấp thông tin của hệ thống máy EP_User đến EP_Server.

Bước 1a : EP_Server sẽ kiểm tra EP_User đã join domain hay chưa.

- Nếu đã join domain, EP_Server sẽ kiểm tra domain đó có trong danh sách domain EPS_Server biết hay không. Nếu domain đó nằm trong danh sách, EP_Server sẽ kiểm tra EP_User đó có nằm trong cơ sở dữ liệu của mình hay không. Nếu không thuộc, EP_Server sẽ cấp cho EP_User đó policy dành cho Catalog (Policy chung cho cả LDAP Server). Nếu EP_User đó thuộc, EP_Server sẽ cấp chính xác policy do Admin chỉ định dành cho user đó. Xem tiếp bước 4.

- Nếu join domain nhưng domain đó không nằm trong database của EP_Server hoặc user đó không join domain. Xem tiếp bước 1b.

Bước 1b : Nếu vẫn chưa xác thực được thông tin của user, EP_Server tiến hành kiểm tra hệ thống xem có hỗ trợ tính năng Proxy Login Server hay không (EP_Server sẽ đóng vai như Proxy Login Server) LDAP Server sẽ là Authentication Server. Xem tiếp bước 2. Nếu không hỗ trợ Proxy Login Server thì EP_Server sẽ cấp Default Policy cho EP_User.

Bước 2 : EP_Server yêu cầu EP_User cung cấp thông tin xác thực.

Bước 3 : EP_User cung cấp thông tin xác thực đến EP_Server (username và encrypted password).

Bước 3a : EP_Server gửi thông tin cần xác thực đến LDAP Server (username + cleartext password).

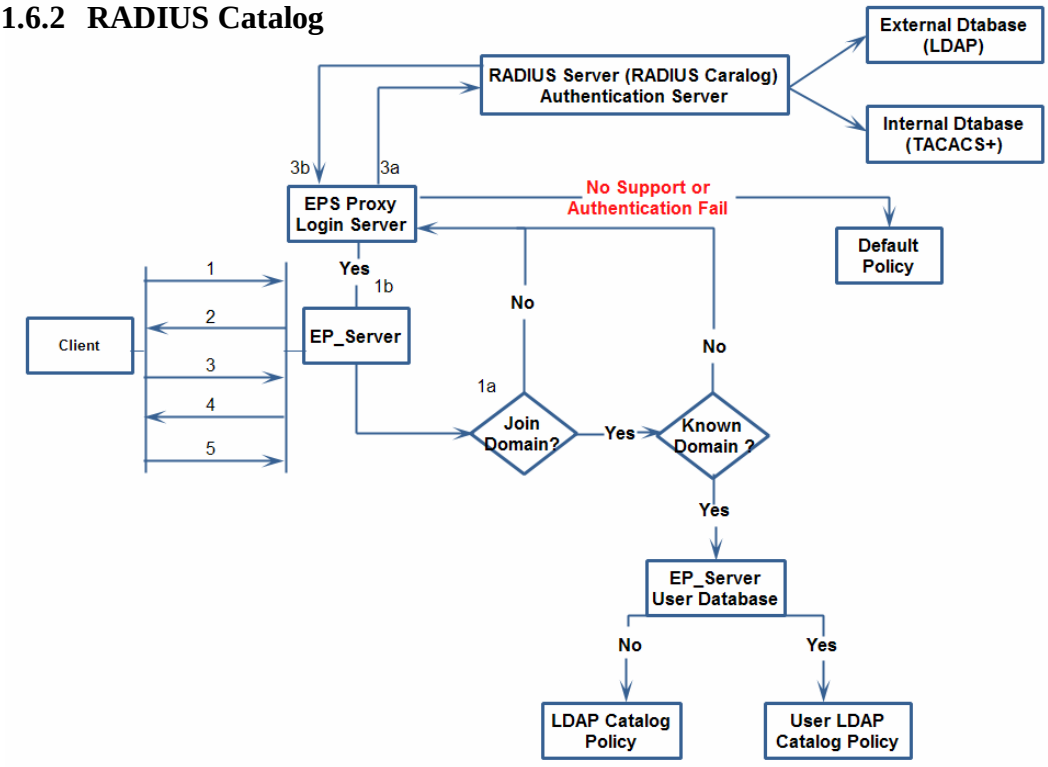
Bước 3b : LDAP Server sẽ xác thực và trả về kết quả cho EP_Server.

Bước 4 : EP_Server cung cấp link để tải Policy.

- Nếu EP_User được xác thực thành công, EP_Server cung cấp link tải Policy dành cho EP_User đó (do Admin chỉ định).
- Nếu EP_User không xác thực thành công. EP_Server sẽ cấp link tải Defaul policy về cho EP_User.

Bước 5 : EP_User Get Policy thông qua giao thức HTTP và cập nhật vào hệ thống.

1.6.2 RADIUS Catalog



Hình C2 – 2 : RADIUS Catalog Authentication Process.

Bước 1 : EP_User khởi tạo kết nối đến EP_Server cung cấp thông tin của hệ thống máy EP_User đến EP_Server.

Bước 1a : EP_Server sẽ kiểm tra EP_User đã join domain hay không.

- Nếu đã join domain, EP_Server sẽ kiểm tra domain đó có trong danh sách domain EP_Server biết hay không. Nếu domain đó nằm trong danh sách, EP_Server sẽ kiểm tra EP_User đó có nằm trong cơ sở dữ liệu của mình hay không. Nếu không thuộc, EP_Server sẽ cấp cho EP_User đó policy dành cho Catalog (policy chung cho cả LDAP Server). Nếu EP_User đó thuộc, EP_Server sẽ cấp chính xác policy do Admin chỉ định dành cho EP_User đó. Xem tiếp bước 4.
- Nếu join domain nhưng domain đó không đồng bộ với EP_Server hoặc EP_User đó không join domain. Xem tiếp bước 1b.

Bước 1b : Nếu vẫn chưa xác thực được thông tin của EP_User, EP_Server tiến hành kiểm tra hệ thống xem có hỗ trợ tính năng Proxy Login Server hay không (EP_Server sẽ đóng vai như Proxy Login Server), lúc này RADIUS Server sẽ là Authentication Servers. Xem bước 2. Nếu không hỗ trợ Proxy Login Server thì EP_Server sẽ cấp Default Policy cho EP_User.

Bước 2 : EP_Server yêu cầu EP_User cung cấp thông tin xác thực.

Bước 3 : EP_User cung cấp thông tin xác thực đến EP_Server (username + encrypted password).

Bước 3a : EP_Server gửi thông tin cần xác thực đến RADIUS Server (username và encrypted password).

Bước 3b : RADIUS Server sẽ xác thực và trả về kết quả cho EP_Server.

Bước 4 : EP_Server cung cấp link để tải Policy.

- Nếu EP_User được xác thực thành công, EP_Server cung cấp link download Policy dành cho EP_User đó (do Admin chỉ định).
- Nếu EP_User không xác thực thành công. EP_Server sẽ cấp link download Defaul policy về cho EP_User.

Bước 5 : EP_User tải Policy dành cho mình thông qua giao thức HTTP và cập nhật vào hệ thống.

2 IP Catalogs

Hỗ trợ việc chỉ định policy đến một EP_user dựa vào địa chỉ IP hoặc Subnet Mask.

C . Managing Security Policy

1 Policy Type

1.1 Enterprise Policy

Khi một máy tính kết nối vào hệ thống mạng, EP_User sẽ tiến hành trao đổi với EP_Server để yêu cầu policy dành cho mình. Và policy được EP_Server cung cấp cho EP_User gọi là Enterprise Policy.

Có hai loại : Connected Enterprise Policy và Disconnected Enterprise Policy.

- Connected Enterprise Policy : Là policy được thực thi khi EP_User có thể kết nối với EP_Server hoặc có thể liên lạc đến địa chỉ được định sẵn trong Office Awareness. Policy này không những bảo vệ hệ thống khỏi các nguy cơ bị tấn công, mà còn đảm bảo các hệ thống máy tính trong mạng được quản lý và thực thi đúng những chính sách bảo mật đã đề ra.
- Disconnected Enterprise Policy : Là policy được thực thi khi EP_User không kết nối được với EP_Server hoặc địa chỉ được định sẵn trong Office Awareness. Policy này cung cấp sự bảo vệ tối thiểu cho hệ thống máy EP_User.

Khi EP_User không thể kết nối được với EP_Server hoặc địa chỉ trong Office Aware thì Connected policy sẽ ngừng hoạt động, và Disconnected policy sẽ được kích hoạt.

Khi EP_User kết nối được vào hệ thống do EP_Server quản lý thì Connected policy sẽ được kích hoạt và Disconnected policy sẽ ngừng hoạt động.

Mục đích của Disconnected policy chính là đảm bảo hệ thống EP_User luôn có được sự bảo vệ cơ bản trước những nguy cơ bị tấn công.

Chúng ta có thể đưa cả hai policy này vào chung một policy pakage hoặc có thể chỉ chọn Connected policy.

Nhằm nâng cao tính linh hoạt cho EP_User, ta có thể sử dụng phiên bản EP_Flex để người dung có thể tự định nghĩa policy cho riêng mình, và không cần thiết phải sử dụng Disconnected policy.

Nếu EP_user sử dụng EP_Flex, thì EP_User sẽ áp dụng cả hai policy (bao gồm Enterprise policy và Personal policy và tất cả những traffic nào rơi vào một trong hai policy này thì EP_User sẽ tiến hành loại bỏ hoặc cho phép tùy theo cấu hình). Vì thế, ta có thể thay đổi thông số để EP_User chỉ thực thi Enterprise policy.

Đối với EP_Agent, nhằm tăng tính bảo mật, ta có thể kết hợp Disconnected policy cho các Remote User và các thiết bị di động ở những thời điểm họ không kết nối được với EP_Server.

1.2 Personal Policy

Khi sử dụng EP_Flex, EP_Users có thể tự định nghĩa Personal policy cho riêng mình (Agent không thể tự định nghĩa policy cho riêng mình). EP_Flex cung cấp nhiều sự tương tác hơn cho người dùng trong việc cấu hình các chính sách bảo mật cho hệ thống khi không chịu sự quản lý của EP_Server (không kết nối vào mạng được quản lý).

EP_Agent không hỗ trợ giao diện tương tác về Personal policy, và Personal policy của EP_Agent là trống, chỉ có thể chỉnh sửa thông qua những tập tin cấu hình.

Khi không nhận được bất kì Enterprise policy nào, tự động Personal policy được kích hoạt cho tới khi nhận được Enterprise policy cấp từ EP_Server.

1.3 Policy Arbitration

Nếu EP_Users dùng EP_Flex đã định nghĩa riêng cho mình một Personal policy, thì policy này sẽ bị hạn chế khi xảy ra có nhiều hơn hai policy hoạt động cùng lúc. Arbitration xảy ra với cả connected và disconnected Enterprise policy (để làm được việc này cần phải chỉnh sửa thông tin Enfoce quá trình thực thi policy ở tab Enforcement Policy).

1.4 Policy Package

Policy package bao gồm hai loại policies được gom chung lại nhằm mục đích nâng cao độ bảo mật cho hệ thống. Sử dụng policy package, ta có thể chỉ ra policy nào thực thi như là Connected policy, hoặc là Disconnected policy (Mỗi policy được chỉ định là Connected policy hoặc Disconnected policy sẽ bao gồm những thành phần security sau : xem phần Policy Component Overview và Policy Object).

1.5 Rule Evaluation and Precedence

Do policy là một tập hợp nhiều loại rule (Firewall rule, Zone rule, Program rule…), nên hoàn toàn có thể xảy ra trường hợp các rule này sẽ xung đột với nhau. Ví dụ Firewall rule sẽ block tất cả các traffic đến port 80, tuy nhiên Zone rule lại cho phép traffic đến port 80, kết quả các traffic port 80 sẽ bị loại bỏ. Vậy để giải quyết vấn đề này, cần phải có một sự phân biệt độ ưu tiên giữa các rule.

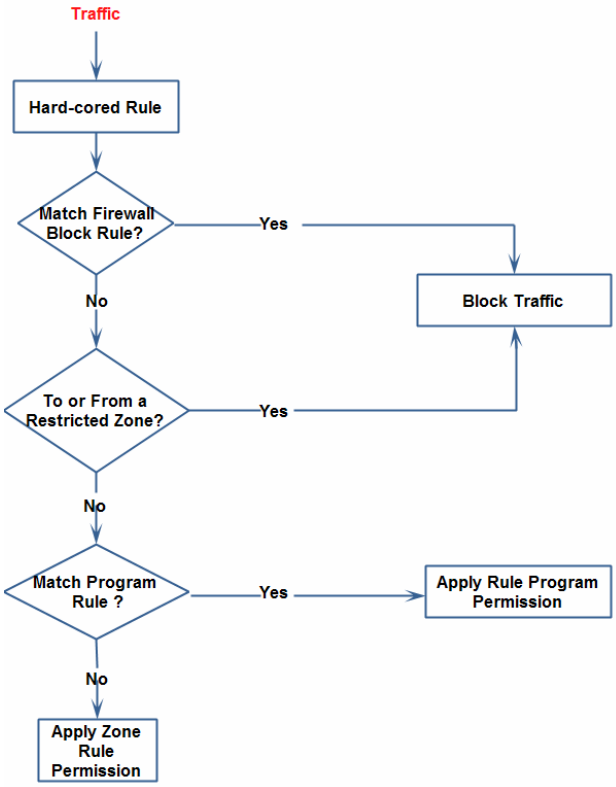
1.5.1 Hard-Cored Rule

Rule này được ưu tiên thực thi trước tất cả các rule khác, và rule này mặc định được tạo ra và không hiển thị trong Endpoint Security Administrator Console. Ta có thể tự thay đổi thông số của Hard-Cored rule bằng cách thay đổi nội dung tập tim XML Policy, tuy nhiên việc này được khuyến khích không nên làm.

- Cho phép UDP packets đến và được khởi tạo từ EP_Server port 80.
- Cho phép TCP packets đến và được khởi tạo từ EP_Server port 443.
- Cho phép traffic từ EP_Users đến port 53 của tất cả các hệ thống máy khác. Rule này cho phép truy xuất dịch vụ DNS.
- Accept ICMP type 9 đến các máy EP_Users. Rule này cho phép sự quảng cáo của Router.
- Loại bỏ tất cả các traffic có địa chỉ nguồn không nằm trong Trusted Zone hoặc Internet Zone (Còn gọi là Clean-up Rule).

1.5.2 Security Rules

Hard-cored Rule được thực hiện trước hết, sau đó Enterprise và Personal policy sẽ được thực thi.



Hình C3 – 1 : Rule Order Process

- EP_User so sánh với các rule của Firewall rules.
  - Nếu Firewall rule định nghĩa loại bỏ traffic này, traffic sẽ bị loại bỏ.
  - Nếu không có bất kì policy nào của Firewall rule loại bỏ traffic này thì quá trình kiểm tra tiếp theo được thực hiện.
- EP_User kiểm tra những traffic đến và được khởi tạo đi từ loại Zone nào.
  - Nếu traffic đến từ Zone bị hạn chế (Blocked Zone), traffic đó sẽ bị loại bỏ.
  - Nếu traffic không bắt nguồn từ Zone bị hạn chế, quá trình kiểm tra tiếp theo được thực hiện.
- EP_User kiểm tra Program rules.
  - Nếu traffic nằm trong danh sách policy của program rule, EP_User thực thi program rule dành cho traffic đó.
  - Nếu traffic không nằm trong danh sách policy của program rule, EP_User sẽ thực thi Zone rule.

2 Creating Policy

2.1 Creating Policy Using Template

Những Template này được tạo từ System-Domain và được sử dụng cho tất cả các Domain khác. Mặc định, Check Point tạo ra ba Template, ta có thể tự tạo một Template

khác phù hợp với hệ thống của mình rồi phổ biến cho tất cả các Domain. Mặc định có 3 loại được cấp sẵn : High, Medium, Observation.

- High Security : Đối với mức này, EP_Users sẽ nhận được nhiều thông báo hơn, tất cả những mạng mới mà EP_Users phát hiện được thì policy sẽ cho rằng mạng đó thuộc vùng Internet Zone và để mức bảo mật cho vùng đó là High Level. Tất cả các traffic từ vùng mạng mới này sẽ bị loại bỏ hoàn toàn (cấu hình mặc định cho vùng Internet Zone là ở mức độ High Level được đề cập ở phần Security Level). Do đó cần phải cập nhật những địa chỉ tin tưởng vào vùng Trusted Zones. Tuy nhiên đối với EP_Flex, họ có thể tự thay đổi thông tin ở vùng Trusted Zone trong Personal policy, vì thế đối với những EP_Users thuộc diện cần được bảo vệ ở mức cao hoặc ít hiểu biết về bảo mật nên triển khai hệ thống EP_Agent. Tính chất Program rule được sử dụng để hạn chế sự giao tiếp mạng của các chương trình trên hệ thống máy EP_Users và môi trường mạng mà Users đó có thể kết nối (Trusted và Internet network).
- Medium Security : Policy này cung cấp sự bảo vệ ít hơn, ít tác động đến quá trình sử dụng của EP_Users. Khi phát hiện ra một mạng mới, policy sẽ mặc định mạng đó thuộc vùng Trusted Zone, và đồng thời tất cả các chương trình sẽ chịu sự quản lý của EP_Server, có toàn quyền giao tiếp vào hệ thống mạng. Tuy nhiên các chương trình này không thể đóng vai như một Application Server.
- Observation : Policy này được thiết kế cho quá trình giám sát các hoạt động của EP_Users và các chương trình trên hệ thống của EP_Users. Policy này cung cấp độ bảo mật ở mức thấp, cho phép các tất cả các traffic không bị hạn chế khi giao tiếp với hệ thống mạng. Tất cả những chương trình giao tiếp mạng đóng vai như Application Client hoặc Application Servers (xem phần Security Program).

2.2 Creating Policy Using File

Được import từ file định dạng XML. Để có được file XML này bằng cách sử dụng tiện ích "export" ở Tab policy manager (trong trường hợp ta lấy policy ở một EP_Server khác).

- Security Level
  - High Level : Mặc định loại bỏ tất cả các traffic và port (traffic của các giao thức TCP, UDP, ICMP, DNS, DHCP…). Tuy nhiên ta vẫn có thể thiết lập để policy có thể bỏ qua port của một số giao thức (TCP/UDP port).
  - Medium Level : Cho phép hầu hết các traffic của các giao thức, bên cạnh đó ta có thể thiết lập để policy chặn port của một số giao thức (TCP/UDP port).
  - Low Level : Tất cả các traffic đều được cho phép.
- Security Program
  - Application Server : Chương trình được quản lý đóng vai như một Server, có thể lắng nghe các traffic truy vấn và trả lời các truy vấn đó.
  - Application Client : Chương trình được quản lý đóng vai như một Client, không cho phép lắng nghe các traffic truy vấn, sẽ loại bỏ tất cả các traffic truy vấn đến port được chương trình đó sử dụng. Có thể gửi gói tin truy vấn dịch vụ đến các hệ thống khác.

3 Policy Object

3.1 Access Zone

Sử dụng Access Zone để chỉ định sự phân biệt về quyền truy xuất giữa các mạng ở hệ thống EP_Users tham gia.

Zone Rule cho phép ta xây dựng mức độ bảo mật (hạn chế, cho phép traffic) dựa vào địa chỉ nguồn và địa chỉ đến của traffic. EP_User phân tích những traffic đến hoặc gửi đi từ hệ thống máy của EP_User bao gồm địa chỉ IP, ports, hoặc giao thức của traffic đó (TCP/UDP). Nếu Program Control được kích hoạt, các traffic đến và gửi đi của các chương trình trên hệ thống máy EP_User cũng sẽ được kiểm tra.

Ta có thể tự thiết lập những thông số của Security Level để phù hợp với nhu cầu, bao gồm

- Protocols : Danh sách các giao thức mặc định mà Checkpoint cung cấp.
- Incoming : Là những traffic mà hệ thống EP_User sẽ nhận, ở mục này ta có thể cho phép hoặc loại bỏ traffic đó.
- Outgoing : Là những traffic mà hệ thống EP_User sẽ gửi đi, ở mục này ta có thể cho phép hoặc loại bỏ traffic đó.
- Đối với những giao thức TCP, UDP ta có thể sử dụng port (ví dụ : 24,25), port range (24-37), hoặc kết hợp cả port và port range (22,23,28-35).

Access Zone sử dụng những thông số sau:

- Host/Site : Địa chỉ trang web.
- IP address : Địa chỉ xác định.
- IP range : Dãy địa chỉ.
- IP Subnet mask : Cả một Subnet.

Access Zone chia làm 3 dạng chính : Trusted Zone, Blocked Zone và Internet Zone. Mặc định, tất cả những traffic đều thuộc vùng Internet Zone.

- Trusted Zone : Vùng này bao gồm những traffic được xem là an toàn và tin tưởng, cho phép trao đổi thông tin với hệ thống EP_User tuy nhiên vẫn có thể bị hảnh hưởng bởi Firewall rule và Program rule. Những traffic cần được đưa vào vùng Trusted Zone bao gồm

  + Những Remote host kết nối vào hệ thống máy EP_User.

  + Hệ thống mạng WAN/LAN được EP_User kết nối.

  + Check Point EP_Server.

  + DNS Servers.

  + Local NIC loopback.

  + Internet Gateway.

  + Local Subnet.

- Blocked Zone : Được xem là nguy hiểm đối với hệ thống vàtất cả những traffic xuất phát từ vùng này sẽ bị loại bỏ tại hệ thống EP_User.
- Internet Zone : Những traffic xuất phát từ vùng này là những traffic được gửi đi từ những địa chỉ chưa được chỉ định trong Trusted Zone và Blocked Zone.

Khi một hệ thống mạng mới được phát hiện bởi EP_User, sẽ có ba lựa chọn cho việc xác định vùng cho hệ thống mạng này

- Include the network in Trusted Zone : Đưa hệ thống mạng này vào vùng Trusted Zone đối với hệ thống EP_User. Và được xem là vùng tin tưởng, được quản lý bởi Trusted Zone policy.
- Leave the network in the Internet Zone : Đưa hệ thống mạng này vào vùng Internet Zone ở EP_Client. Và được quản lý bởi Internet Zone policy.
- Ask the Flex End-point User : Nếu EP_User sử dụng EP_Flex, EP_User có quyền chỉ định vùng cho hệ thống mạng đó trong Personal policy. Tuy nhiên đối với EP_Agent thì hệ thống mạng này sẽ được đưa vào vùng Internet Zone. Và mạng này vẫn sẽ chịu ảnh hưởng bởi độ ưu tiên về policy, sử dụng Enterprise Policy được nếu policy này đang được kích hoạt.

3.2 Firewall Rule

3.2.1 Firewall Rule Overview

Sử dụng Firewall Rule nhằm hạn chế hoặc cho phép các hoạt động mạng dựa trên những thông tin kết nối bao gồm địa chỉ IP, ports, protocols, quá trình kiểm tra dựa trên cả hai hướng incoming và outgoing, bao gồm

- Kết hợp những thông số tạo nên một hệ thống Firewall trên hệ thống máy EP_User.
- Tinh chỉnh, quản lý các chương trình bằng cách hạn chế sự truy xuất mạng của một hay nhiều chương trình dựa vào quá trình quản lý các giao thức.
- Hạn chế và ngăn chặn các sự truy xuất hoặc giao tiếp bất hợp pháp.

3.2.2 Firewall Rule Rank

Rank được sử dụng trong Firewall Rule nhằm đánh dấu thứ tự rule nào sẽ được sử dụng để kiểm tra traffic.

Khi các thông số của traffic được kiểm tra trùng với các thông số trong rule, thì rule đó được thực thi và ngừng việc kiểm tra traffic đó.

Ta có thể thay đổi Rank nhằm phù hợp với mục đích của mình.

Name	Rank	Source	Destination	Protocol	Time	Action	Track
Web Access Remove | Disable	1 Change ▾	Client Computer	web1.hoasen.edu.vn	Web Servers HTTP	Always	Allow	None
WEB_Other Remove | Disable	2 Change ▾	Client Computer	Any	Web Servers HTTP	Always	Block	None

Hình C3 – 2 : Example 1 – Cho phép truy xuất Web1.hoasen.edu.vn

Name	Rank	Source	Destination	Protocol	Time	Action	Track
WEB_Other Remove | Disable	1 Change ▾	Client Computer	Any	Web Servers HTTP	Always	Block	None
Web Access Remove | Disable	2 Change ▾	Client Computer	web1.hoasen.edu.vn	Web Servers HTTP	Always	Allow	None

Hình C3 – 3 : Example 2 – Loại bỏ các traffic truy xuất giao thức HTTP

3.2.3 Firewall Rule Parameter

Nếu Firewall rule được tạo ở System Domain (trong Multi-Domain mode) thì rule đó sẽ là Global rule, và sẽ xuất hiện trong tất cả các option của danh sách Firewall rule trong các Domain khác.

Nếu Firewall rule được tạo trong một Non-System Domain thường thì rule đó chỉ mang giá trị Local rule, và chỉ tồn tại trong domain đó.

3.3 Enforcement Rule

Sử dụng Enforcement Rule nhằm đảm bảo hệ thống của EP_Users phải đáp ứng được những yêu cầu về tiêu chuẩn bảo mật tối thiểu để được xem như là an tòan (tiêu chuẩn do Admin đề ra) khi tham gia vào hệ thống mạng, bao gồm hệ thống Anti-Virus, Anti-Spyware hoặc một số bản vá lỗi của hệ điều hành… Nếu hệ thống EP_Users không đáp ứng được những yêu cầu này, ta có thể hạn chế sự kết nối của EP_Users thông qua Restrict rule được tích hợp trong Enforcement rule.

Bên cạnh đó, Enforcement rule có thể yêu cầu cài đặt hoặc loại bỏ các chương trình trên hệ thống máy EP_Users tuy nhiên lại không quản lý các hoạt động của các chương trình này. Để quản lý các hoạt động của chương trình, sử dụng Program Rule.

3.3.1 Enforcement Rule Types Overview

❖ General Enforcement Rule

Chỉ định những giá trị (registry) hoặc tập tin (bao gồm vị trí của tập tin đó, phiên bản, thời gian tập tin đó được chỉnh sửa, tính integrity của tập tin…) là những giá trị hoặc tập tin được yêu cầu phải có hoặc không được phép tồn tại trên hệ thống của EP_Users.

Ví dụ : Yêu cầu từ EP_User khi đăng nhập vào hệ thống, nếu Operating System của EP_User là XP thì phải là cài đặt bản Hotfix KB898461. Hệ thống của EP_User khi tham gia vào hệ thống sẽ được kiểm tra sự tồn tại của giá trị này trong Registry tại vị trí

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP3\KB898461
```

❖ Anti-Virus Rule

Sử dụng rule này kiểm tra nhằm đảm bảo hệ thống EP_Users phải có một chương trình Anti-Virus được Checkpoint tin tưởng là an toàn. Nếu không đáp ứng được chính sách về loại engine và database của chương trình Anti-virus do Admin chỉ định, EP_Users sẽ ở trang thái “out-of compliance”.

❖ Client Rule

Những quy định về EP_Client Package ở hệ thống của EP_Users (bao gồm version EP_Client package, database của Anti-virus…).

❖ Rule Group

Nếu ta có một loạt những quy định, tuy nhiên chỉ yêu cầu Users thỏa mãn một trong các quy định đó, thì ta có thể sử dụng Rule Groups để thực hiện việc này.

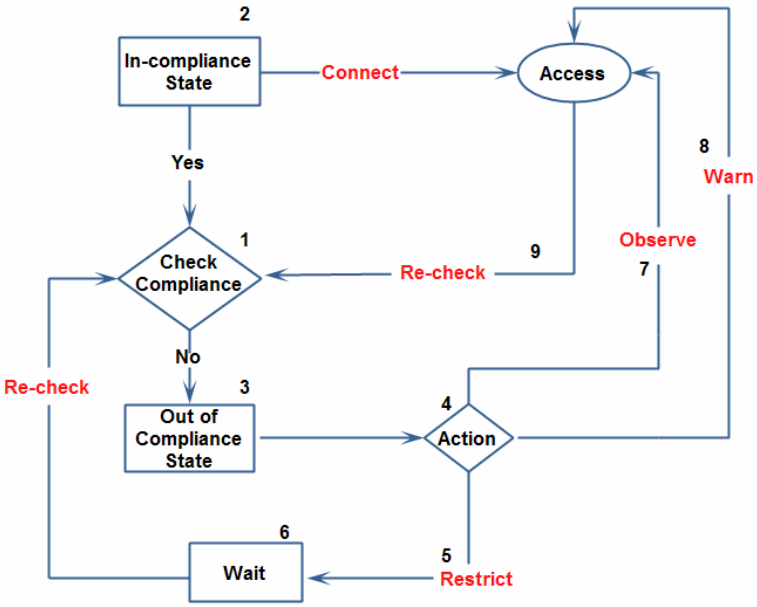
Ví dụ : Phần mềm Anti-Virus bao gồm Kaspersky, Avira, Panda…chỉ cần EP_Users có một trong những chương trình này thì đáp ứng được yêu cầu về Anti-virus Enforcement Rule.

Tuy nhiên, tất cả các rule trong group đó chức năng Auto Remediation sẽ không được kích hoạt, và ta có thể cung cấp Remediation Resource bằng Sandbox (trang web hỗ trợ các EP_Users khi không đáp ứng về các chính sách bảo mật của hệ thống).

Nếu một rule trong group đó hỗ trợ Auto Remediation được gán cho một policy khác không phải dưới dạng group thì rule đó vẫn có chức năng Auto Remediation.

❖ **Enforcement Rule Process**

EP_Users thường xuyên được kiểm tra hệ thống để đảm bảo hệ thống đó luôn đáp ứng được các chính sách của Enforcement rule, nếu hệ thống EP_Users không đáp ứng được những quy định này thì các Restrict rule được định nghĩa trong Enforcement rule sẽ được thực thi.



Hình C3 – 4 : Enforcement Rule Process

Bước 1 : EP_User tiến hành kiểm tra những Enforcement rule trong policy, bao gồm cả Anti-virus Provider rule và groups.

Bước 2 : Nếu hệ thống EP_User đáp ứng được các quy định của Enforcement rule, hệ thống đó được xem là "Compliance" (hợp pháp), và tất cả các kết nối của EP_User được tiếp tục hoạt động bình thường.

Bước 3 : Nếu hệ thống EP_User không đáp ứng được các quy định của Enforcement rule, hệ thống đó được xem là "out-of compliance".

Bước 4 : Khi không đáp ứng được các quy định, EP_User tiến hành thực thi các các hạn chế trong Enforcement rule, trong trường hợp này ta có thể tùy chọn điều chỉnh trạng thái bảo mật của EP_User chỉ có thể là Observer, Warn (cảnh báo) đến EP_User, hoặc là Restrict "hạn chế" các kết nối của hệ thống EP_User.

Bước 5 : Các rule "Restrict" này sẽ được thực thi trước khi những rule trong Firewall rule được thực thi.

Bước 6 : Nếu chọn "Observer" hoặc "Warn", việc thực thi sẽ xảy ra lập tức, đối với "Restrict" hành động này sẽ xảy ra sau một giới hạn (Threshold) do số lần "Heartbeats" mặc định là 4 lần (Heartbeats là gói tin chứa những thông tin về trạng thái và tính hợp pháp (compliance) của hệ thống EP_User gửi về cho EP_Server thông qua giao thức UDP port 6054 sau một khoảng thời gian nhất định, mặc định là 60 giây). Dựa vào số lần "Heartbeats" này để thực hiện việc "Restrict" hệ thống EP_user.

Bước 7 : Khi hệ thống EP_User ở trạng thái "Observer", EP_User vẫn được tham gia hệ thống mạng tuy nhiên tất cả các hoạt động đó đều được lưu lại.

Bước 8 : Khi hệ thống EP_User ở trạng thái "Warn", EP_User vẫn được tham gia hệ thống mạng, tất cả các hoạt động đều được lưu lại, và sẽ được thông báo (alert) về các quy định của Enforcement rule mà EP_User không đáp ứng được, đồng thời cũng cung cấp đường dẫn hỗ trợ thông tin để khắc phục tình trạng này (Sandbox).

Bước 9 : Các EP_Client sẽ liên tục kiểm tra EP_user để đảm bảo policy luôn được thực thi chính xác.

3.3.2 Remediation Resource and Sandbox

Remediation Resource được sử dụng trong các Enforcement Rule, Anti-virus Enforcement Rule, Client Enforcement Rule.

Khi EP_User "out-of compliance" và các Enforcement rule được thực thi, việc cung cấp thông tin khắc phục cho Giúp hệ thống EP_user trở nên "compliance" vô cùng quan trọng. Những thông tin này gọi là "Remediation Resource". Bên cạnh việc cung cấp những thông tin cảnh báo (alert) về phần mềm hoặc một tập tin nào đó không đáp ứng được yêu cầu, ta có thể cung cấp đường dẫn đến hệ thống hướng dẫn EP_User khắc phục lỗi.

Sandbox được xem như một hệ thống hỗ trợ các EP_Users khi ở trạng thái "out-of compliance". Ở trang web này, ta sẽ cung cấp những nguyên nhân dẫn đến lí do làm EP_Users rơi vào trạng thái out-of compliance. Đối với mỗi loại chính sách đều được xây dựng một trang web riêng bao gồm những nguyên nhân liên quan đến chính sách đó. Bên cạnh đó đưa ra những hướng dẫn giúp EP_Users khắc phục lỗi.

Bên cạnh đó, ta có thể cung cấp Remediation Resource bởi Sandbox, giúp cung cấp cho EP_Users nhiều thông tin chính xác và nâng cao kiến thức về chính sách bảo mật của hệ thống cho EP_Users.

3.3.3 Enforcement Rule Parameter

Chỉ định những giá trị registry hoặc tập tin (bao gồm vị trí của tập tin đó, phiên bản, thời gian tập tin đó được chỉnh sửa, tính integrity của tập tin) là những giá trị hoặc thông tin được yêu cầu phải có hoặc không được phép tồn tại trên hệ thống của EP_User.

- Rule name : Tên của Enforcement rule.
- Operating System : Version của hệ điều hành Windows (2000/2003/0XP/Vista).
- Check for registry key and value : Chỉ định giá trị key cần có trong registry của hệ thống EP_User và giá trị của key đó.
- Check for file and properties : Yêu cầu kiểm tra sự tồn tại và thông số của một tập tin trên hệ thống EP_User. Cung cấp tên của tập tin đó (ví dụ : firefox.exe) và những thông số của tập tin đó.
- Running at all times.
- Location : Đường dẫn đến tập tin đó (bao gồm cả tập tin, ví dụ : c:/firefox.exe).
- Version number.
- Laste modified less than “n” days ago.
- Match Smart Checksum : Kiểm tra giá trị checksum của chương trình trong máy EP_User với giá trị Admin cung cấp.
- Type of Check : Chỉ định yêu cầu đối với tập tin đó “cần thiết” (require) và “ngăn cấm” (prohibit).
- Action : Hành động
  - Observe Clients that don’t comply : Log các hoạt động, tuy nhiên Users vẫn tham gia hệ thống mạng bình thường.
  - Warn Clients that don’t comply : Hiện thị cảnh báo đến EP_Users là đang bị “out-of compliance”. User vẫn tham gia hệ thống mạng bình thường.
  - Restrict Clients that don’t comply : Thực thi Restrict rule và gửi thông báo đến EP_User.

Đối với hai dạng War và Restrict action, ta nên hỗ trợ EP_Users “out-of compliance” bằng cách chọn option Remediation Resource và Sandbox”.

3.3.4 Anti-virus Enforcement Rule Parameter

Sử dụng rule này kiểm tra nhằm đảm bảo hệ thống EP_Users phải có một chương trình Anti-Virus được Checkpoint tin tưởng. Nếu không đáp ứng được yêu cầu này, EP_User sẽ ở trang thái “out-of compliance”. Ta có thể gửi thông báo và đưa ra biện pháp khắc phục cho EP_User thông qua “Remediation Resource”.

Khi tạo một Anti-virus provider rule, ta có thể yêu cầu dựa theo Anti-virus engine và cơ sở dữ liệu (Signature-based) của chương trình đó.

- Minimum engine version : Yêu cầu về phiên bản của chương trình Anti-virus tồn tại trên hệ thống EP_User ít nhất phải bằng với version được quy định.

- Minimum DAT file version : Yêu cầu phiên bản Signature-based của chương trình Anti-virus trên hệ thống EP_User ít nhất phải bằng version được quy định.
- Oldest DAT file time stamp : Yêu cầu phiên bản Signature-based của chương trình Anti-virus trên hệ thống EP_User phải bằng với version được quy định.
- Maximum DAT file age, in "x/day" : Thời gian cập nhật của Signature-based của chương trình Ati-virus sẽ được so với thời gian cập nhật của hệ thống EP_Server, nếu chênh lệch "x" day thì EP_User sẽ bị xem là "out-of compliance". (Ví dụ : Signatured-based version của Kaspersky Anti-virus được cập nhật trên EP_Server là ngày 20/12, mà ở hệ thống của EP_User là 15/12, nếu ta chỉ định x=2 thì hệ thống EP_User sẽ không đáp ứng được yêu cầu, và sẽ rơi vào trạng thái "out-of compliance".

Việc cập nhật thông tin về engine cũng như cơ sở dữ liệu virus của chương trình Anti-virus cho các policy có thể được thực hiện thủ công hoặc tự động. Đối với phương pháp tự động, engine và Signature-based version mà EP_Server sẽ đồng bộ với Reference Clients (hệ thống máy cài đặt chương trình Anti-virus mà EP_Server sẽ đồng bộ để lấy thông tin về Engine và Signature-based version), và EP_Server sẽ dùng những thông tin này để kiểm tra tính "compliance" của EP_User.

3.4 Anti-virus and Anti-spyware Rules

Ta có thể chỉ định yêu cầu thực thi tiến trình quét toàn bộ hệ thống tại một thời điểm định sẵn. Đối với spyware, do mức độ ảnh hưởng cấp Network, do đó việc thực thi nghiêm túc yêu cầu quét toàn bộ hệ thống bởi Anti-spyware rất cần thiết, do đó ta có thể Restrict EP_User đó nếu yêu cầu này không được thực hiện. Đối với virus, ta có thể cho tiến trình tự động quét tại một thời điểm nhất định, và không có điều kiện cho việc thực hiện tiến trình quét virus.

Ta có thể chỉ định những đối tượng cần được quét (Local, Removable, CD-ROM…) đồng thời cũng có thể chỉ định bỏ qua tiến trình kiểm tra những tập tin được định sẵn.

3.5 Program Control Rules

Khác với Firewall, hạn chế quá trình truy xuất dựa vào lớp Network (mô hình TCP/IP) bao gồm source, destination IP, port, time, khác với Zone hạn chế quá trình truy xuất dựa vào nguồn gọi là Location mà ta định sẵn.

Program Rule cung cấp cho Admin khả năng hạn chế quá trình truy xuất giao tiếp mạng của mỗi chương trình có chức năng ứng dụng mạng (Ex_program) được chỉ định trên hệ thống EP_Users.

Program Rule không quy định một chương trình nào đó được hoặc không được cài đặt trong hệ thống (xem Enforcement Rule), mà chỉ có thể quản lí quá trình truy xuất mạng của chương trình đó.

Program Rule gồm ba thành phần : Observation, Permission, Advisor.

3.5.1 Program Observation

Program Observation cho phép Admin lấy những thông tin về các Ex_program được sử dụng trên hệ thống của EP_Users. Khi EP_Server có được những thông tin về

Ex_program này, Admin có thể áp đặt quy định để điều khiển quá giao tiếp mạng của chương trình ở các hệ thống của EP_User. Tuy nhiên Program Observation sẽ mặc định được kích hoạt ở EP_User, thành phần này không xuất hiện trong Endpoint Security Administrator Console. Khi EP_Server nhận những thông tin về Ex_program do Program Observation gửi đến, nếu Ex_program đó không có trong cơ sở dữ liệu của Program Advisor và Program do Admin định sẵn (cập nhật thủ công) thì Ex_program đó sẽ được đưa vào phần Unknown Program.

Ta có thể quy định thời gian mà Program Observation sẽ cung cấp thông tin về các Ex_program trên hệ thống EP_User, tuy nhiên tại một thời điểm nào đó EP_User cài đặt và sử dụng một Ex_program, tuy nhiên chưa đến lúc Program Observation gửi thông tin của Ex_program này đến cho EP_Server, do đó ta có định nghĩa Reference program : là những Ex_program được quản lý bởi EP_Server đã được cập nhật trong cơ sở dữ liệu. Đối với những Ex_program mà EP_Server chưa cập nhật trong Reference program thì được xem là Unknown program, và chờ đợi sự truy vấn từ EP_server đến Program Advisor Server (nếu có) để cập nhật permission về program này, nếu Program Advisor Server hỗ trợ program này thì nó sẽ tự động cập nhật vào group Program Advisor terminated program hoặc Program Advisor Reference program (xem phần Program Advisor), nếu Program Advisor Server không hỗ trợ thì nó sẽ được giữ lại trong group Unknown program và Admin sẽ tự điều chỉnh permission cho nó hoặc sẽ sử dụng permission của group Unknown sử dụng để quản lý program này.

3.5.2 Program Permission

Program Permission cho phép Admin có thể hạn chế quá trình tham gia vào hệ thống mạng của Ex_program, bao gồm

- Zone : Program Permission sẽ đánh giá traffic được gửi hoặc nhận của một Ex_program từ vùng Trusted hoặc vùng Internet.
- Role : Program Permission sẽ đánh giá vai trò của chương trình đó khi thực hiện hoặc nhận các kết nối từ hệ thống mạng ngoài bao gồm vùng Internet và Trusted.
    - Internet Zone/Act as Client : Ex_program sẽ có vai trò như một hệ thống Client khi thực hiện các kết nối với các hệ thống thuộc vùng Internet. Ex_program sẽ chỉ có thể thực hiện các yêu cầu truy vấn mà sẽ không đáp trả lại các yêu cầu truy vấn từ các hệ thống thuộc vùng Internet.
    - Internet Zone/Act as Server : Ex_program sẽ có thể lắng nghe các truy vấn từ các hệ thống thuộc vùng Internet, và có thể đáp trả lại các yêu cầu đó.
    - Trusted Zone/Act as Server : tương tự Internet Zone/Act as Server tuy nhiên đối tượng lại là những hệ thống từ Trusted Zone.
    - Trusted Zone/Act as Client : tương tự Internet Zone/Act as Server tuy nhiên đối tượng lại là những hệ thống từ Trusted Zone.

3.5.3 Program Advisor

Program Advisor (PA) là một tính năng cung cấp Program Permission bởi Checkpoint dành cho các Ex_program, cơ sở dữ liệu về các loại Ex_program này được

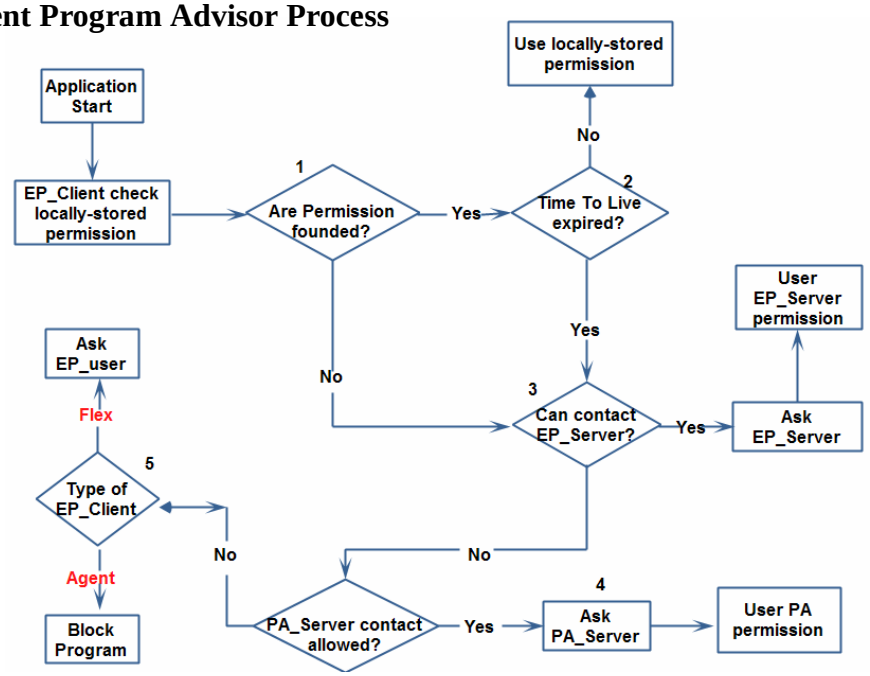
quản lý bởi Checkpoint. Khi tính năng Program Advisor hoạt động, Program Observation phát hiện những Ex_program được đặt trên hệ thống EP_User, nó sẽ gửi những thông tin này về cho EP_Server và EP_Server sẽ truy vấn đến Program Advisor central (Checkpoint Server). Tuy nhiên nếu EP_User không thể kết nối đến EP_Server thì EP_User sẽ trực tiếp gửi yêu cầu đến cho PA, và nếu EP_User không thể nhận được bất cứ hỗ trợ nào từ EP_Server và PA thì EP_User sẽ dùng permission dành cho Unknown program để áp dụng trong trường hợp này.

Tuy nhiên, ta có thể tự thay đổi Permission được cung cấp bởi Checkpoint để phù hợp với hệ thống mạng của mình. Program Advisor gồm hai loại là Terminated program và Reference program.

- Terminated program : Là những Ex_program mà Checkpoint khuyến cáo nên loại bỏ tất cả những traffic được tạo bởi nó.
- Referenced program : Là những Ex_program thông thường, ít nguy cơ bị tấn công và có thể quản lý bằng chính sách, Checkpoint có cung cấp sẵn một tiêu chuẩn chính sách cho mỗi Ex_program.

Tiến trình làm việc của hệ thống Program Advisor bao gồm Client Program Advisor Process và Server Program Advisor Process.

❖ **Client Program Advisor Process**



Hình C3 – 5 : Client Program Advisor Process

Bước 1 : Ex_program được kích hoạt bởi user, EP_User sẽ kiểm tra program permission dành cho Ex_program đó trong Policy package đang tồn tại trên hệ thống EP_User (bao gồm Enterprise policy và Personal policy).

Bước 2 : Nếu khi permission dành cho Ex_program đó được tìm thấy trong locally-stored permission, EP_User sẽ kiểm tra giá trị Expired time. Nếu chưa expired, EP_User sẽ sử dụng permission này để quản lý Ex_program. Nếu đã expired, EP_User sẽ gửi yêu cầu truy vấn tới

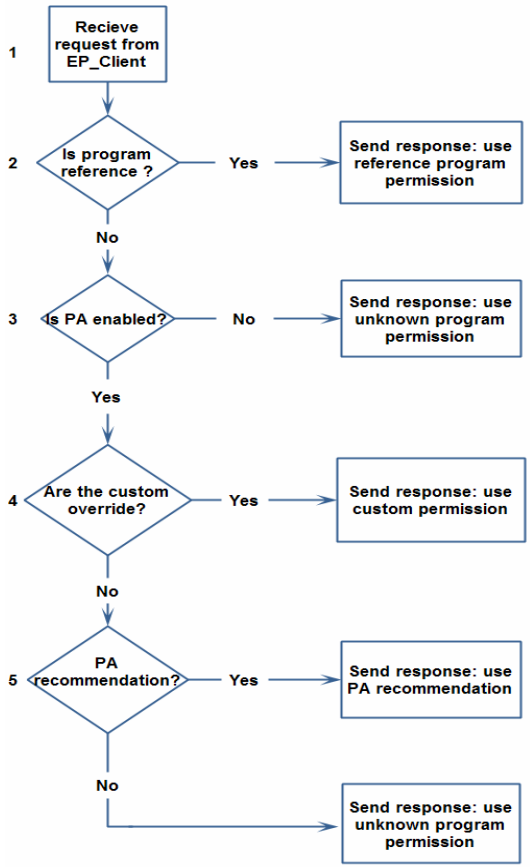
EP_Server, yêu cầu EP_Server cung cấp permission dành cho Ex_program đó, sau khi nhận được policy permission mới từ EP_Server, EP_User sẽ sử dụng chính sách quản lý đó để đối với Ex_program.

Bước 3 : Nếu EP_User không thể tìm thấy permission trong locally-stored permission, nó sẽ truy vấn tới EP_Server yêu cầu cung cấp chính sách quản lý dành cho Ex_program đó. Sau khi nhận được chính sách quản lý từ EP_Server, EP_User sử dụng chính sách đó để quản lý Ex_program.

Bước 4 : Trường hợp EP_User ở bước 2 và 3 đều không thể liên lạc được với EP_Server, EP_User sẽ tiến hành liên lạc với Prgoram Advisor Server nếu được cho phép, và nhận permission từ Program Advisor Server.

Bước 5 : Trường hợp EP_User ở bước 2 và 3 đều không thể liên lạc được với EP_Server và EP_User cũng không được phép liên lạc hoặc không thể liên lạc được với Program Advisor và EP_Server, nếu EP_User là phiên bản EP_Flex thì EP_User sẽ truy vấn Personal Policy về chính sách quản lý dành cho Ex_program này. Đối với phiên bản EP_Agent, mặc định tất cả traffic được gửi đi và nhận bởi Ex_program đó sẽ không được cho phép.

❖ **Server Program Advisor Process**



Hình C3 – 6 : Server Program Advisor Process

EP_Server nhận truy vấn về program permission từ EP_User, kết hợp với Program Advisor Server, EP_Server sẽ nhận được những hỗ trợ về program permission (từ Program Advisor Server) nên sử dụng đối với Ex_program để cung cấp cho EP_User yêu cầu.

Bước 1 : EP_Server nhận được truy vấn từ EP_User yêu cầu cung cấp program permission về một Ex_program.

Bước 2 : EP_Server kiểm tra xem Ex_program này đã có tồn tại trong Reference program chưa (dựa vào mã MD5 Checksum). Nếu permission dành cho Ex_program này đã tồn tại trong Reference, thì EP_Server sẽ gửi chính sách quản lý này về cho EP_User. Và EP_Usert sẽ cập nhật permission này vào Enterprised policy.

Bước 3 : Trường hợp Ex_program này không thuộc Reference program, ở EP_server, Ex_program sẽ được đưa vào group Unknown program, nếu tính năng Program Advisor không được kích hoạt, EP_Server sẽ gửi permission của group Unknown program (do Admin tự chỉ định) về cho EP_User.

Bước 4 : Nếu tính năng Program Advisor được cho phép sử dụng, nếu Ex_program đó đã được cập nhật vào Reference program của EP_Server thông qua Program Advisor Server, EP_Server sẽ gửi chính sách quản lý của Ex_program đó về cho EP_User. Đối với chính sách quản lý được cung cấp từ Program Advisor Server ta có thể tùy chỉnh thay đổi những thông số trong permission đó để linh hoạt trong việc quản lý Ex_program. Hoặc sử dụng chính chính sách đó.

Bước 5 : Trường hợp tính năng Program Advisor được cho phép sử dụng, đồng thời Ex_program chưa có trong Reference program hoặc thời gian hiệu lực của chính sách đó trên EP_Server đã hết, EP_Server sẽ truy vấn Program Advisor Server yêu cầu cấp mới chính sách cho Ex_program đó. Nếu Ex_program này được hỗ trợ từ Program Advisor Server, EP_Server sau khi nhận được chính sách sẽ cập nhật lại expired time trong Reference program hoặc cập nhật vào Program Advisor Terminated program (nếu CheckPoint cho rằng đây là Ex_program cần cấm triệt để) hoặc Program Advisor Reference program (Checkpoint cho rằng đây là Ex_program phổ biến, có thể hạn chế nguy hiểm). Nếu Ex_program này quá mới, Program Advisor Server chưa có thông tin về program này, thì EP_Server sẽ đưa program này vào group Unknown program và gửi chính sách quản lý (do Admin tự chỉ định) về cho EP_User.

3.6 Smart-Defense

Smart-Defense cung cấp một hệ thống bảo vệ trước những cuộc tấn công DoS vào hệ thống của EP_User. Smart-Defense là chương trình hoạt động độc lập ở hệ thống EP_Users, được đưa vào trong EP_Client package. Chức năng này được kích hoạt qua Enterprise policy được cung cấp từ Admin. Tuy nhiên, chức năng này không hoạt động hiệu quả. Và dần được thay thế bởi các chức năng Anti-virus, Anti-spyware.

D . Gateway and Cooperative Enforcement

1 Cooperative Enforcement Overview

Nhằm đảm bảo hệ thống mạng được quản lý chặt chẽ, các chính sách bảo mật được thực thi nghiêm túc trước những công nghệ di động ngày càng tiên tiến (Laptop, SmartPhone…) rất khó cho việc quản lý sự truy xuất thông tin của các hệ thống này, công nghệ Cooperatvie Enforcement được sử dụng nhằm ngăn chặn, kiểm tra tính hợp pháp và quản lý các Users khi cố gắng tham gia và hệ thống mạng ở bất cứ đâu (thiết bị Switch, Access Point, Firewall, Router,…). Sử dụng Cooperative Enforcement, ta có thể xây dựng những yêu cầu chính sách bảo mật cơ bản nhất ở hệ thống của mỗi EP_Users khi tham gia vào hệ thống mạng được bảo vệ, bao gồm

- Hệ thống EP_Users phải được cài đặt EP_Client package, bao gồm một hệ thống bảo mật cơ bản : Anti-spyware, Anti-virus, Firewall.
- Được quản lý và kiểm tra bởi các chính sách dành cho EP_Users khi tham gia vào hệ thống.
- Có khả năng tương tác với hệ thống quản lý tập trung EP_Server.

Với công nghệ Cooperative Enforcement, ta có thể hạn chế những hoạt động của EP_Users khi tham gia vào hệ thống qua những Gateway (Access Point, Firewall, Switch, Router,…). Nhanh chóng kiểm tra tính hợp pháp của EP_User trước khi EP_User đó được tham gia vào hệ thống mạng, bảo vệ các hệ thống trong mạng trước sự lây lan từ các hệ thống mới có độ bảo mật thấp khi tham gia và hệ thống mạng. Bên cạnh đó hỗ trợ khả năng quản lý hạn chế sự truy xuất bất hợp pháp, lưu thông tin log phục vụ cho quá trình kiểm tra nếu cần.

2 Network Access Server Integration

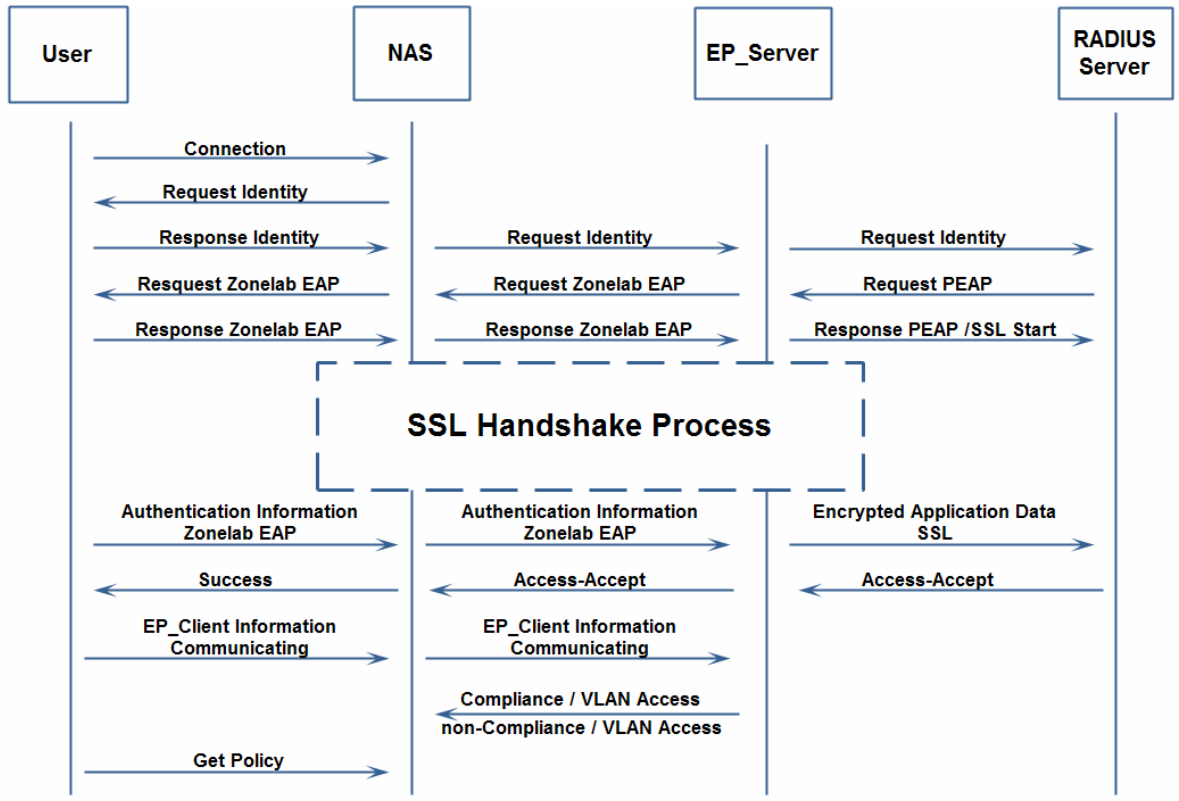
Switch đóng vai trò rất quan trọng trong hệ thống mạng, hỗ trợ nhiều port cho các hệ thống máy có thể kết nối với nhau, tuy nhiên đối với công nghệ di động ngày càng phát triển, ta có thể sử dụng Laptop để có thể truy xuất vào nhiều Switch một cách bất hợp pháp, NAS sẽ giúp hệ thống Switch và EP_Server tương tác với nhau nhằm có thể quản lý các hành động của EP_Users.

2.1 Cooperative Enforcement Architecture

Mô hình hệ thống Network Access Server (NAS) bao gồm

- Switch (Catalyst 2950) : Là thiết bị NAS, có nhiệm vụ thực hiện yêu cầu xác thực các hệ thống EP_User khi khởi tạo kết nối tham gia vào mạng thông qua Switch với phương thức xác thực là 802.1x. Trong mô hình Cooperative với EP_Server, Switch sẽ tiếp nhận những yêu cầu của EP_Server và gửi đến cho EP_User. Đồng thời cho phép EP_Server chỉ định VLAN cho từng port mà EP_User kết nối (nếu thiết bị NAS có hỗ trợ).
- EP_Server : Đóng vai là một RADIUS Proxy Client, thực hiện nhiệm vụ thay mặt EP_User xác thực với RADIUS Server, đồng thời đảm bảo tính “compliance” của EP_User khi tham gia vào hệ thống mạng.

- RADIUS Server : Là Authentication Server.
- User : EP_User cần tham gia hệ thống mạng thông qua phương thức 802.1x.



Hình C4 – 1 : NAS Workflow

2.2 Cooperative Enforcement Workflow

Bước 1 : EP_User sẽ tạo một kết nối đến NAS.

Bước 2 : NAS yêu cầu EP_User thực hiện quá trình xác thực Request Identity (cung cấp username + password).

Bước 3 : EP_User cung cấp username và password (tuy nhiên chỉ username được gửi đi).

Bước 4 : NAS tiến hành gửi yêu cầu xác thực đến EP_Server.

Bước 5 : EP_Server tiến hành gửi yêu xác thực đến RADIUS Server.

Bước 6 : RADIUS Server kiểm tra thông tin, và thực hiện yêu cầu EP_Server sử dụng phương thức PEAP cho quá trình xác thực (bằng gói tin Access-Challenge).

Bước 7 : EP_Server tiến hành kiểm tra tính "compliance" của user (yêu cầu hệ thống EP_User phải cài đặt EP_Client package) bằng cách gửi về cho NAS và yêu cầu sử dụng phương thức xác thực là Zonelab EAP (EAP Type method 44), và NAS gửi về cho EP_User.

Bước 8 : EP_User sẽ gửi lại cho NAS với thông tin được sử dụng theo phương thức xác thực kiểu Zonelab EAP, nếu EP_User không cài đặt EP_Client package thì EP_User sẽ không đáp ứng được yêu cầu này, EP_User sẽ gửi gói Legacy NAK không đáp ứng được phương pháp xác thực này đến cho NAS.

Bước 9 : NAS gửi thông tin đến cho EP_Server, nếu EP_User không đáp ứng được yêu cầu, EP_Server sẽ tiến hành "Reject" quá trình xác thực của EP_User đồng thời hủy phiên xác thực với RADIUS Server.

Bước 10 : Nếu EP_User đáp ứng được yêu cầu từ EP_Server, EP_Server sẽ đại diện cho EP_User tiến hành tạo kết nối SSL với RADIUS server.

Bước 11 : Sau khi hoàn thành phiên kết nối, EP_User tiến hành gửi thông tin xác thực đến RADIUS Server (thông qua NAS và EP_Server) và RADIUS Server tiến hành xác thực trả về cho EP_Server, EP_Server sẽ dựa vào thông tin này để yêu cầu NAS cho phép EP_User đó được vào VLAN nào (VLAN access, VLAN restrict: do EP_Server quyết định).

Bước 11a : Nếu user xác thực thành công (Access-Accept), EP_Server có thể trao đổi thông tin với EP_User để kiểm tra tính "compliance". Bên cạnh việc ta có thể restrict một EP_User thông qua Enterprise Policy, thì EP_Server có thể yêu cầu NAS chuyển port kết nối của EP_User (compliance) vào VLAN Access, và của EP_User (non-compliance) vào VLAN restrict (các VLAN này sẽ do nhà quản trị chỉ định).

Bước 11b : Nếu EP_User xác thực không thành công, EP_Server sẽ gửi "Reject" về cho NAS, và NAS thông báo về cho EP_User, phiên kết nối bị hủy. Và khởi tạo yêu cầu xác thực mới đến EP_User sau khoảng thời gian xác định.

KINH NGHIỆM VÀ KHÓ KHĂN

Kinh Nghiệm

Dù gặp nhiều khó khăn trong Khóa Luận Tốt Nghiệp này, nhưng chúng tôi đã cố gắng hết sức để có thể hoàn thành tốt nhất những gì đã được đề ra. Và thông qua những khó khăn đó, chúng tôi đã có được nhiều hơn những kiến thức và kinh nghiệm thực tế để xử lý các trục trặc, khó khăn trong quá trình xây dựng và quản trị hệ thống bảo mật.

- Có được kinh nghiệm nhiều hơn trong việc tìm kiếm thông tin và xác định nguồn thông tin nào đáng tin tưởng.
- Kinh nghiệm sử dụng các phần mềm hỗ trợ như eDraw, VMWare…
- Kinh nghiệm phân tích, xử lý gói tin được bắt bằng WireShark.
- Kinh nghiệm sử dụng và cấu hình các phần mềm OPSEC của Checkpoint.
- Kinh nghiệm cấu hình Active Directory Application Mode của Windows.
- Kinh nghiệm làm việc nhóm nghiêm túc, phân chia bình đẳng, hỗ trợ lẫn nhau để cả nhóm có kiến thức như nhau.
- Nâng cao kỹ năng giao tiếp ngôn ngữ chuyên ngành bằng tiếng Anh và trình độ chuyên môn bằng các cuộc đối thoại "Live Chat" với Checkpoint's Advisors.
- Kinh nghiệm viết báo cáo theo chuẩn ISO 5966.

Khó khăn

Trong suốt quá trình thực hiện Khóa Luận Tốt Nghiệp này, chúng tôi đã cố gắng hết sức để thực hiện thật tốt bài báo cáo, song vẫn không tránh khỏi những sai sót và những khó khăn.

Trước tiên là quá trình thực hiện Khóa Luận Tốt Nghiệp của chúng tôi không hề được hỗ trợ về mặt thiết bị thật cũng như thiết bị chuyên dụng, tất cả mọi thứ đều được thực hiện ở thiết bị ảo trên một máy tính duy nhất. Do đó quy mô những bài thực hành của chúng tôi khá nhỏ, không thể bao quát tất cả các vấn đề vào cùng một bài thực hành.

Bên cạnh đó thì việc sử dụng thiết bị ảo sẽ đi kèm theo một khó khăn là vấn đề về License, một số chức năng không được hỗ trợ, chức năng bị lỗi hoạt động không ổn định hoặc có hỗ trợ nhưng không thể sử dụng.

Thời gian thực hiện Khóa Luận Tốt Nghiệp so với những vấn đề chúng tôi nghiên cứu là khá ngắn, nên chúng tôi không thể đi sâu hơn vào các vấn đề. Nếu có thể cho chúng tôi thêm thời gian thì những nội dung của Khóa Luận Tốt Nghiệp có thể sẽ hay hơn.

Chúng tôi đã không sử dụng được những ứng dụng thực tế với độ bảo mật cao và tiên tiến (Như RSA SecureID, SMS Gateway Authentication, …) vì vấn đề License cũng như giá cả của thiết bị.

PHỤ LỤC

A . Bảng giá đề nghị

Trường hợp 1 : Sử dụng Appliances

Trong trường hợp này thì các thiết bị chính của hệ thống là các thiết bị Appliances. Hai thiết bị Appliances cần mua là Security Gateway và Connectra. Ngoài ra còn có Licenses cho các Endpoint(EP) Client.

- Security Gateway CPAP-SG576 : 8,408.50
- Connectra CPWS-CRA-M9072-2500 : 73,391.68

❖ **Tổng cộng : 81,800.18**

- EP Server Licences CPEP-SA-1-100TO4999 : 37.27$ per User
- EP On Demand 2500User (Optional) CPWS-CCV-2500 : 11,182.91

Trường hợp 2 : Sử dụng Sotfware

Trong trường hợp này thì ta sẽ mua các gói phần mềm thay vì sử dụng Applicances. Ưu điểm là có khả năng mở rộng phần cứng. Tuy nhiên tính ổn định sẽ không bằng các thiết bị Appliances.

- Security Bundle CPSG-P405-CPSM-P1003 : 14,161.75
- Connectra Software CPWS-CRS-2500 : 60,078.77

❖ **Tổng cộng : 74,240.52**

- EP Server Licences CPEP-SA-1-100TO4999 : 37.27$ per User
- EP On Demand 2500User (Optional) CPWS-CCV-2500 : 11,182.91

Chi tiết các thiết bị

❖ **Security Gateway : Check Point UTM-1 576 Total Security Appliance**

- SKU : CPAP – SG576
- Price : 8,408.50 $
- MSRP : 10,900 $
- 10/100/1000 Ports : 6
- Fiewall Throuhput : 2.5Gbps
- VPN Throughput : 300Mbps
- IPS Throughput : 1.7Gbps
- Concurrent Sessions : 650,000
- Licensed User : Unlimited
- Storage : 160GB
- Enclosure : 1U

- Software Blade : Firewall, VPN, IPS, Anti-Spam & Email Security, URL Filtering, Anti-Virus & Anti-Malware
- Management Blade : Network Policy Management, Endpoint Policy Management, Logging & Status

❖ **Connectra : Check Point Connectra 9072 appliance for 2500 Concurrent Users**

- SKU : CPWS-CRA-M9072-2500
- Price : 73,391.68 $
- MSRP : 95,000 $
- Concurrent Users : 2,500
- Licensed User : Unlimited
- Storage : 160GBx2
- Enclosure : 2U

❖ **Security Bundle CPSG-P405-CPSM-P1003**

- SKU : CPSG-P405-CPSM-P1003
- Price : 14,161.75 $
- MSRP : 19,000 $
- Including : SG405 and SM1003
- SG405 Including : Including Firewall, IPSec VPN, Advanced Networking, Acceleration & Clustering and IPS
- SM1003 : Network Policy Management, Endpoint Policy Management, Logging & Status.

❖ **Connectra : Check Point Connectra software for 2500 Concurrent Users**

- SKU : CPWS-CRS-2500
- Price : 60,078.77 $
- MSRP : 85,000 $

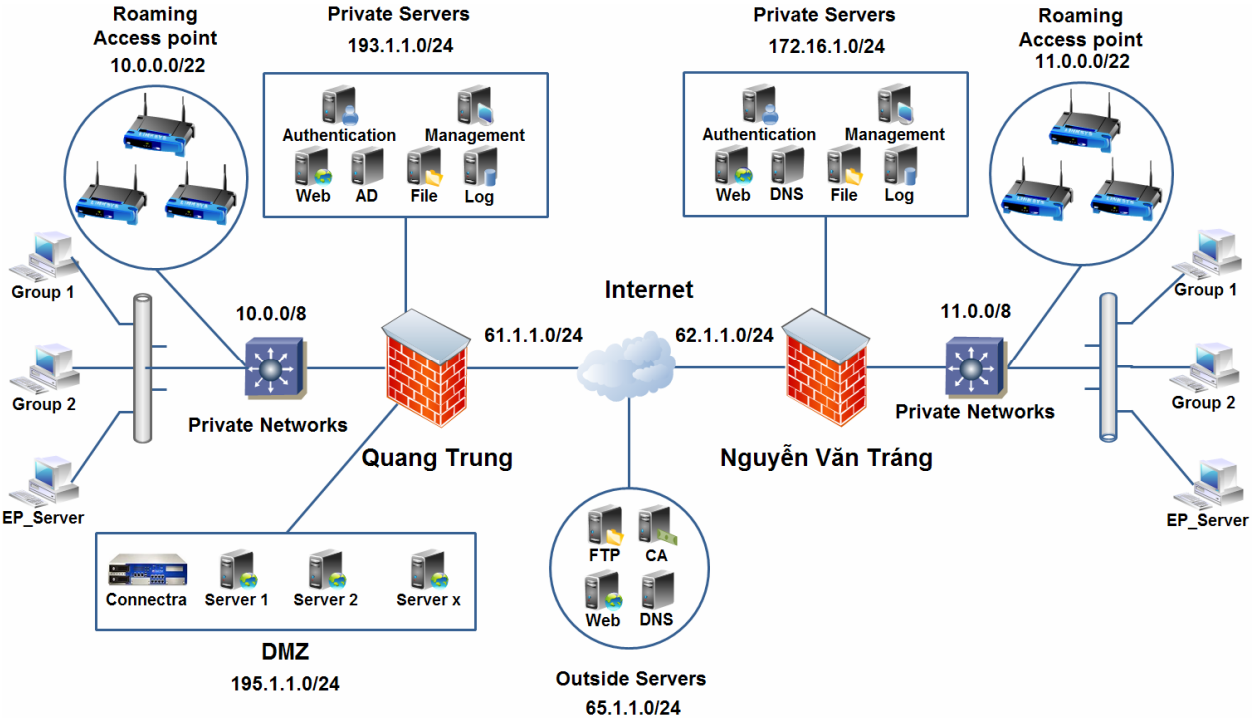
❖ **EP Server Licences CPEP-SA-1-100TO4999**

- SKU : CPEP-SA-1-100TO4999
- Price : 37.27 $
- MSRP : 50 $

❖ **EP On Demand 2500User (Optional) CPWS-CCV-2500**

- SKU : CPEP-SA-1-100TO4999
- Price : 11,182.91 $
- MSRP : 15,000 $

B . Sơ đồ mạng Hoa Sen đề nghị



C . Tổng hợp Rule

1 Firewall Rule

Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS | Desktop

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	Users => Connectra	Any	Connectra	Any Traffic	Connectra_Protocols	accept	None	QT	Any
2	Users => DMZ	Any	DMZ	Any Traffic	TCP https TCP http	accept	Log	QT	Any
3	Stealth	Any	QT	Any Traffic	Any	drop	Log	QT	Any
4	DNS	QT_Network	DNS-Server	Any Traffic	dns	accept	None	QT	Any
5	Clientless	Clientless-Group@Any	Internal_Web_Server	Any Traffic	TCP https	User Auth	Log	QT	Any
6	Connectra Authentication	Connectra	Authentication_Server	Any Traffic	Authentication_Protocols	accept	Log	QT	Any
7	Connectra => Internal	Connectra	Internal_Server	Any Traffic	Connectra_to_Internal	accept	Log	QT	Any
8	Join Domain	LAN_QT	Active_Directory	Any Traffic	Join_Domain_Protocols	accept	None	QT	Any
9	EP_Server Authentication	EP_Server	Authentication_Server	Any Traffic	Authentication_Protocols	accept	Log	QT	Any
10	Remote Users=>EP_Server	VPN-Group@Any	EP_Server	RemoteAccess	EP_Client_Protocols	accept	None	QT	Any
11	Remote Users => Internal	VPN-Group@Any	LAN_QT	RemoteAccess	TCP http	accept	Log	QT	Any
12	Site-to-Site	QT_VPN_Group	NVT_VPN_Group	IPsec	TCP http	accept	None	QT	Any
13	LAN => Management	LAN_QT	Management	Any Traffic	Any	drop	None	QT	Any
14	LAN => Internet	LAN_QT	Any	Any Traffic	TCP http	accept	None	QT	Any
15	Clear	Any	Any	Any Traffic	Any	drop	Log	QT	Any

Hình E5 – 1 : Firewall

Rule 1 : Cho phép Remote Users có thể truy cập vào Connectra. Bao gồm các Services

- HTTPS (TCP 443)
- CP_SSL_Network_Extender (TCP 444)
- IKE_NAT_TRAVERSAL (UDP 4500)

Rule 2 : Cho phép Users (LAN, Internet) có thể truy cập vào vùng DMZ.

Rule 3 : Stealth Rule sẽ ngăn chặn việc truy cập trực tiếp vào Security Gateway.

Rule 4 : DNS cho phép các mạng của Quang Trung có thể truy vấn DNS, bao gồm

- LAN_QT
- Management
- DMZ
- Security Gateway

Rule 5 : Cho phép Users có thể sử dụng Clientless VPN.

Rule 6 : Cho phép Connectra có thể kết nối tới Authentication Server (RADIUS, TACACS+, ADAM, AD…).

Rule 7 : Cho phép Connectra có thể kết nối tới Internal Server.

- Web Application : HTTP (TCP 80)
- Fileshare Application : Microsoft-ds (TCP/UDP 445)
- Mail Exchange : IMAP (TCP 143), SMTP (TCP 25)
- Native Application : Telnet (TCP 23), Remote Desktop (TCP 3389), …

Rule 8 : Cho phép các Users trong LAN_QT có thể Join Domain.

Rule 9 : Cho phép EP_Server có thể kết nối tới Authentication Server (RADIUS, TACACS+, ADAM, AD…).

Rule 10 : Cho phép Remote Users có thể trao đổi thông tin với EP_Server.

Rule 11 : Cho phép Remote Users hợp lệ có thể truy cập đến mạng Internal.

Rule 12 : Quản lý kết nối IPsec Site-to-Site VPN từ Nguyễn Văn Tráng tới Quang Trung.

Rule 13 + 14 : Cho phép Users ở vùng LAN_QT có thể truy cập Internet. Tuy nhiên hạn chế các truy cập bất hợp pháp vào vùng Management.

Rule 15 : Cho phép log lại những truy cập không được cho phép bởi những Rule trên.

2 NAT Rule

Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS | Desktop

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	* Any	Public_Address	http	= Original	Internal_Server	= Original	QT
2	Connectra	* Any	* Any	Connectra (Valid	= Original	= Original	QT
3	* Any	Connectra (Valid Address)	* Any	= Original	Connectra	= Original	QT
4	LAN_QT	LAN_QT	* Any	= Original	= Original	= Original	QT
5	LAN_QT	* Any	* Any	LAN_QT (Hiding .	= Original	= Original	QT
6	Remote_Pool	Remote_Pool	* Any	= Original	= Original	= Original	QT
7	Remote_Pool	* Any	* Any	Remote_Pool (Hic	= Original	= Original	QT

Hình E5 – 2 : NAT Firewall

Rule 1 : Cho phép Public các Internal Server trong vùng DMZ ra Internet (Static NAT).

Rule 2 + 3 : Cho phép Remote Users ở Internet có thể truy cập vào Connectra (Automatic NAT).

Rule 4 + 5 : Cho phép Users ở LAN_QT có thể truy cập Internet (Automatic NAT).

Rule 6 + 7 : Cho phép Remote Users sử dụng IPsec Remote Access VPN (Office Mode và Hub Mode) có thể truy cập Internet (Automatic NAT).

3 Endpoint Security Rule

Quy tắc đặt Rule : ***Action*** *Source → Destination : Service.*

3.1 "Public" Policy Public

- Đối tượng : Desktop PC và Laptop.
- Phương pháp xác thực : Join Domain hoặc 802.1x.
- Quản lý bằng User Catalog.
- Software : Endpoint Agent Client Package (Tích hợp Antivirus, Spyware).
- IP Range : 10.0.1.1 → 10.0.5.254
- Firewall Rule
  - Permit User → Active_Directory : Join_Domain_Protocol
  - Deny User → Active_Directory : Any
  - Permit User → FTP_Server : FTP, HTTP
  - Deny User → FTP_Server : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Deny User → EP_Server : Any
  - Deny User → Authentication_Server : Any
- Access Zone (Medium Security)
  - Trusted Zone : 10.0.1.1 → 10.0.5.255
  - Blocked Zone : 10.0.0.1 → 10.0.1.255
  - Blocked Zone : 10.0.6.1 → 10.255.255.255
  - Blocked Zone : VPN Group
  - Internet Zone
- Program Advisor
  - Không cho sử dụng Torrent, Garena,…
- Enforcement Rule
  - Antivirus Requirement : Group Program (Kaspersky, AVG,…)
  - Enforcemence Rule
    - Win XP : XPSP3(KB936929)
  - Restricted Rule
    - Permit User → kaspersky.nts.com.vn, AVG.com… : Any
    - Permit User → Microsoft.com : Any
    - Permit User → EP_Server : Endpoint_Client_Protocol
    - Permit User → FTP : FTP, HTTP
    - Deny Any → Any : Any
- Client Setting
  - Không cho phép User tắt Endpoint Software.
  - Tắt tường lửa của Windows.
  - Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.2 "Networking Computer Lab"Policy

- Đối tượng : Desktop PC.
- Quản lý bằng Custom và Build-in Package Policy.
- Software : Endpoint Agent Client Package (Không tích hợp Antivirus, Spyware).
- IP Range : 10.0.6.1 → 10.0.10.254 (4 Phòng)
- Firewall Rule
  - Deny User → Active_Directory : Any
  - Deny User → FTP_Server : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Deny User → EP_Server : Any
  - Deny User → Authentication_Server : Any
- Access Zone (Medium Security)
  - Trusted Zone : 10.0.X.1 → 10.0.X.255
  - Blocked Zone : 10.0.1.1 → 10.0.(X-1).255
  - Blocked Zone : 10.0.(X+1).1 → 10.255.255.255
  - Blocked Zone : VPN Group
  - Internet Zone
  - 5<X<11
- Program Advisor
  - Không cho sử dụng Torrent, Garena,…
- Client Setting
  - Không cho phép User tắt Endpoint Software.
  - Tắt tường lửa của Windows
  - Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.3 "Networking Computer Lab – Switch" Policy

- Đối tượng : Laptop.
- Phương pháp xác thực : 802.1x.
- Quản lý bằng User Catalog.
- Software : Endpoint Agent Client Package (Tích hợp Antivirus, Spyware).
- IP Range : 10.0.6.1 → 10.0.10.254 (4 Phòng)
- Firewall Rule
  - Deny User → Active_Directory : Any
  - Deny User → FTP_Server : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Deny User → EP_Server : Any
  - Deny User → Authentication_Server : Any

- ❖ Access Zone (Medium Security)
  - Trusted Zone : 10.0.X.1 → 10.0.X.255
  - Blocked Zone : 10.0.1.1 → 10.0.(X-1).255
  - Blocked Zone : 10.0.(X+1).1 → 10.255.255.255
  - Blocked Zone : VPN Group
  - Internet Zone
  - 5<X<11
- ❖ Program Advisor
  - Không cho sử dụng Torrent, Garena,…
- ❖ Enforcement Rule
  - Antivirus Requirement : Group Program (Kaspersky, AVG,…)
  - Enforcemence Rule
    - Win XP : XPSP3(KB936929)
  - Restricted Rule
    - Permit User → kaspersky.nts.com.vn, AVG.com… : Any
    - Permit User → Microsoft.com : Any
    - Permit User → EP_Server : Endpoint_Client_Protocol
    - Permit User → FTP : FTP, HTTP
    - Deny Any → Any : Any
- ❖ Client Setting
  - Không cho phép User tắt Endpoint Software.
  - Tắt tường lửa của Windows.
  - Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.4 "Computer Lab" Policy

- ❖ Quản lý bằng Custom Catalog và Build-in Package Policy
- ❖ Đối tượng : Desktop PC.
- ❖ Software : Endpoint Agent Client Package (Tích hợp Antivirus, Spyware).
- ❖ IP Range : 10.0.11.1 → 10.0.30.254 (20 Phòng)
- ❖ Firewall Rule
  - Deny User → Active_Directory : Any
  - Deny User → FTP_Server : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Deny User → EP_Server : Any
  - Deny User → Authentication_Server : Any
- ❖ Access Zone (Medium Security)
  - Trusted Zone : 10.0.X.1 → 10.0.X.255
  - Blocked Zone : 10.0.1.1 → 10.0.(X-1).255
  - Blocked Zone : 10.0.(X+1).1 → 10.255.255.255
  - Blocked Zone : VPN Group

- Internet Zone
- 9<X<31

❖ Program Advisor
- Không cho sử dụng Torrent, Garena,…

❖ Enforcement Rule
- Antivirus Requirement : Group Program (Kaspersky, AVG,…)
- Enforcemence Rule
  - Win XP : XPSP3(KB936929)
- Restricted Rule
  - Permit User → kaspersky.nts.com.vn, AVG.com… : Any
  - Permit User → Microsoft.com : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Permit User → FTP : FTP, HTTP
  - Deny Any → Any : Any

❖ Client Setting
- Không cho phép User tắt Endpoint Software.
- Tắt tường lửa của Windows.
- Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.5 "Computer Lab – Switch" Policy

❖ Đối tượng : Laptop.

❖ Phương pháp xác thực : 802.1x.

❖ Quản lý bằng User Catalog.

❖ Software : Endpoint Agent Client Package (Tích hợp Antivirus, Spyware).

❖ IP Range : 10.0.11.1 → 10.0.30.254

❖ Firewall Rule
- Deny User → Active_Directory : Any
- Deny User → FTP_Server : Any
- Permit User → EP_Server : Endpoint_Client_Protocol
- Deny User → EP_Server : Any
- Deny User → Authentication_Server : Any

❖ Access Zone (Medium Security)
- Trusted Zone : 10.0.X.1 → 10.0.X.255
- Blocked Zone : 10.0.1.1 → 10.0.(X-1).255
- Blocked Zone : 10.0.(X+1).1 → 10.255.255.255
- Blocked Zone : VPN Group
- Internet Zone
- 9<X<31

- Program Advisor
  - Không cho sử dụng Torrent, Garena,…
- Enforcement Rule
  - Antivirus Requirement : Group Program (Kaspersky, AVG,…)
  - Enforcement Rule
    - Win XP : XPSP3(KB936929)
  - Restricted Rule
    - Permit User → kaspersky.nts.com.vn, AVG.com… : Any
    - Permit User → Microsoft.com : Any
    - Permit User → EP_Server : Endpoint_Client_Protocol
    - Permit User → FTP : FTP, HTTP
    - Deny Any → Any : Any
- Client Setting
  - Không cho phép User tắt Endpoint Software.
  - Tắt tường lửa của Windows
  - Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.6 "Staff" Policy

- Đối tượng : Desktop PC và Laptop.
- Phương pháp xác thực : Join Domain hoặc 802.1x.
- Quản lý bằng User Catalog.
- Software : Endpoint Agent Client Package (Tích hợp Antivirus, Spyware).
- Đối tượng : Desktop PC (Xác thực : Join Domain) và Laptop (Xác thực 802.1x)
- IP Range : 10.0.50.1 → 10.0.50.255
- Firewall Rule
  - Permit User → AD : Join_Domain_Protocol
  - Deny User → AD : Any
  - Permit User → FTP_Server : FTP
  - Deny User → FTP : Any
  - Permit User → EP_Server : Endpoint_Client_Protocol
  - Deny User → EP_Server : Any
  - Deny User → Authentication_Server : Any
- Access Zone (Medium Security)
  - Trusted Zone : 10.0.X.1 → 10.0.X.255
  - Blocked Zone : 10.0.1.1 → 10.0.(X-1).255
  - Blocked Zone : 10.0.(X+1)s.26 → 10.255.255.255
  - Internet Zone
  - 49<X<71
- Program Advisor
  - Không cho sử dụng Torrent, Garena,…

- ❖ Enforcement Rule
  - Antivirus Requirement : Group Program (Kaspersky, AVG,…)
  - Enforcement Rule
    - Win XP : XPSP3(KB936929)
  - Restricted Rule (Firewall Rule 2) :
    - Permit User → kaspersky.nts.com.vn, AVG.com… : Any
    - Permit User → Microsoft.com : Any
    - Permit User → EP_Server : Endpoint_Client_Protocol
    - Permit User → FTP : FTP, HTTP
    - Deny Any → Any : Any
- ❖ Client Setting
  - Không cho phép User tắt Endpoint Software.
  - Tắt tường lửa của Windows
  - Tắt Wireless adapter khi cổng LAN được kết nối vào mạng LAN.

3.7 "Examination" Policy

- ❖ Đối tượng : Desktop PC và Laptop.
- ❖ Phương pháp xác thực : Join Domain hoặc 802.1x.
- ❖ Quản lý bằng User Catalog và Build-in Package Policy.
- ❖ Đối tượng : Desktop PC và Laptop (Xác thực 802.1x)
- ❖ IP Range : 10.0.1.1 → 10.0.49.254
- ❖ Firewall Rule
  - Permit User → EP_SERVER : Endpoint_Client_Protocol
  - Deny Any → Any : Any

❖ **Join_Domain_Protocol**

Port	***Checkpoint Keyword***	***Description***
Port 42 TCP		Host name Service
Port 42 UDP	Name	Host name Service
Port 53 (TCP + UDP)	DNS	DNS
Port 88 TCP	Keberos_v5_TCP	Kerberos
Port 88 UDP	Keberos_v5_UDP	Kerberos
Port 135 TCP		DCE Endpoint Resolution
Port 135 UDP		DCE Endpoint Resolution
Port 137 TCP		Net-BIOS Name Service
Port 137 UDP	nbname	Net-BIOS Name Service
Port 138 TCP		Net-BIOS Datagram Service
Port 138 UDP	nbdatagram	Net-BIOS Datagram Service
Port 139 TCP		Net-BIOS Session Service
Port 139 UDP	nbsession	Net-BIOS Session Service
Port 389 TCP	LDAP	LDAP

Port 389 UDP		LDAP
Port 636 TCP	LDAP-SSL	LDAP-SSL
Port 636 UDP		LDAP-SSL
Port 445 TCP	microsoft-ds	microsoft-ds
Port 445 UDP	microsoft-ds-udp	microsoft-ds
Port 3268 TCP		MS Global Catalog
Port 3268 UDP		MS Global Catalog
Port 3269 TCP		MS Global Catalog with LDAP-SSL
Port 3269 UDP		MS Global Catalog with LDAP-SSL
Port 1025 TCP	Remote_Storm	unassigned

❖ **Endpoint_Client_Protocol**

Port 80/6054 TCP : Heartbeat
Port 443 TCP : SSL
Port 2100 : Trao đổi thông tin giữa khởi động ban đầu.

❖ **Authentication_Protocol**

Port TCP 389 : LDAP
Port TCP 636 : LDAP-SSL
Port UDP 1812 : RADIUS
Port UDP 1813 : RADIUS Accounting
Port UDP 49 : TACACS
Port TCP 49 : TACACS+

D . Tài liệu tham khảo

"Connectra – Central/Local Management – Administration Guide – Version NGX R66"
Check Point Software Technologies Ltd, September 11, 2008

"Connectra – Getting Started Guide – Version NGX R66"
Check Point Software Technologies Ltd, September 9, 2008

"Checkpoint IPS – Administrator Guide – Version R70"
Check Point Software Technologies Ltd, March 8, 2009

C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH"
RFC 2403, November 1998.

C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH"
RFC 2404, November 1998.

C. Madson, N. Doraswamy, "The ESP DES-CBC Cipher Algorithm"
RFC 2405, November 1998.

D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP"
RFC 2407, November 1998.

D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)"
RFC 2408, November 1998.

D. Harkins, D. Carrel, "The Internet Key Exchange (IKE) "
RFC 2409, November 1998.

"Endpoint Security Server – Administration Guide – Version R70"
Check Point Software Technologies Ltd, February 23, 2010.

"Endpoint Security – Gateway Integration Guide – Version R72"
Check Point Software Technologies Ltd, July 21, 2009.

"Endpoint Security – Implementation Guide – Version NGX 7.0 GA"
Check Point Software Technologies Ltd, January 9, 2008.
Computer Network laboratory, "802.1-Wired-Wireless", CN@Lab
http://netlab18.cis.nctu.edu.tw/html/wlan_course/powerpoint/chap-06.pdf

E. Rescorla, "Diffie-Hellman Key Agreement Method"
RFC 2631, June 1999.

Earl Carter, Jonathan Hogue," Intrusion Prevention Fundamentals"
Cisco Press, January 18, 2006.

"Firewall - Administration Guide – Version R70"
Check Point Software Technologies Ltd, March 5, 2009.
Jose Nazario,"Defense and Detection Strategies against Internet Worms",Artech House - Library of Congress Cataloging-in-Publication Data, 2004

James Henry Carmouche ,"IPsec Virtual Private Network Fundamentals"
Cisco Press, July 19, 2006.

Mark Lewis,"Comparing, Designing, and Deploying VPNs"
Cisco Press, April 12, 2006.

S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol"
RFC 2401, November 1998.

S. Kent, R. Atkinson, "IP Authentication Header"
RFC 2402, November 1998.

S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)"
RFC 2406, November 1998.

"Security Management Server – Administration Guide – Version R70"
Check Point Software Technologies Ltd, March 8, 2009.

Vijay Bollapragada, Mohamed Khalid, Scott Wainner, "IPSec VPN Design "
Cisco Press, April 07, 2005.

"Virtual Private Network – Administration Guide – Version R70"
Check Point Software Technologies Ltd, March 1, 2009.

E . Website tham khảo

Checkpoint User Group Forum
http://www.cpug.org/forums/

Cisco System Website
http://www.cisco.com/en/US/hmpgs/index.html

Check Point Software Technologies Ltd Website
http://www.checkpoint.com/

J. H. Carmouche, Network World, Cisco Press, Chapter 4 : Common IPsec VPN Issues
http://www.networkworld.com/subnets/cisco/1114-ch4-ipsec-vpn.html?page=1

Jupiter Network Security Website
http://www.juniper.net/us/en/security/

Google – Internet Searching
http://www.google.com.vn/

Mail-Archive
http://www.mail-archive.com

Offensive Security Website
http://backtrack.offensive-security.com/index.php/Main_Page

Oliver Pell Website
http://www.ridex.co.uk/cryptology/

WikiPedia – The Free Encyclopedia
http://en.wikipedia.org/wiki/Main_Page

Virtual Private Network Consortium Website
http://www.vpnc.org/