Access Control List Network Solution for Cleveland Branch Offices

Kevin O'Neal
DeVry University
NETW208: Accessing the WAN

Submitted to:
Professor: Hopkins
Date: 10.-7-2012

Implementation and Creation of Access Control List

The purpose of this document is to implement the creation of access control lists to aid in the securing of a VPN. To offer an example of a VPN security policy and to show possible examples of ACL rules for this implementation.

About ACL's: Access Control Lists are a basic set of rules created to permit or deny traffic either inbound or outbound of a router. These ACL's are implemented at the interface level. ACL rules pertain to layer 3 packets. They can also be used for layer 4 for filtering. Standard access control lists should be configured nearest the destination device. Extended access control lists are best configured nearest the source of the transmission to be filtered. Inbound ACL's are filtered before they are allowed to traverse the router. Outbound ACL's are routed through the outbound router interface and then filtered by the outbound ACL. ACL's can be numbered or named. They can be configured as Standard, Extended or Complex. Standard ACL's can only filter source IP's of packets. Access control list statements are traversed from the top down and will only be processed until there is a match. ACL's have an implicit "deny all" as a last line. There needs to be at least one permit rule within an ACL or no traffic will be allowed through the interface. One final concept of Access Control Lists is that only one ACL per protocol can be utilized, one ACL per interface is allowed and only one ACL per direction can be configured.

Access List Number Ranges:

Type	Range
IP Standard	1–99
IP Extended	100–199
IP Standard Expanded Range	1300–1999
IP Extended Expanded Range	2000–2699

Named ACLs: To make the documentation of ACL's easier, names can be used in both conventions of access control lists (Standard and Extended). Names must contain alphanumeric characters. It is recommended that ALLCAPS are used to stand out for easy viewing of ACL's. Names can't contain spaces or punctuation. Finally, all ACL names must begin with an alphabetic character.

Final Notes on ACL's: The order of the statements within an ACL is of the utmost importance. The most restrictive statements should be at the top and least restrictive following. If no match is found, the packet will be dropped implicitly. Each ACL needs an unique identifying name or number. A router cannot filter traffic that originated from that router. Applying an empty ACL allows all traffic. To deny all traffic, at least on statement has to be included in the ACL, for the implicit deny to function. Wildcard masks are used to help the router determine which parts of the subnet to look at. To calculate a wildcard mask, one subtracts each byte of the subnet mask from 255.

Implementation

Example of a VPN Security Policy:

Virtual Private Network (VPN) Policy

Created by the SANS Institute. Send e-mail to stephen@sans.edu

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the You Decide Company corporate network.

2.0 Scope
This policy applies to all You Decide Company employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the You Decide Company network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy
Approved You Decide Company employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to You Decide Company internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by You Decide Company network operational groups.
6. All computers connected to You Decide Company internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from You Decide Company's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not You Decide Company -owned equipment must configure the equipment to comply with You Decide Company's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of You Decide Company's network, and as such are subject to the same rules and regulations that apply to You Decide Company owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
IPSec Concentrator	A device in which VPN connections are terminated.

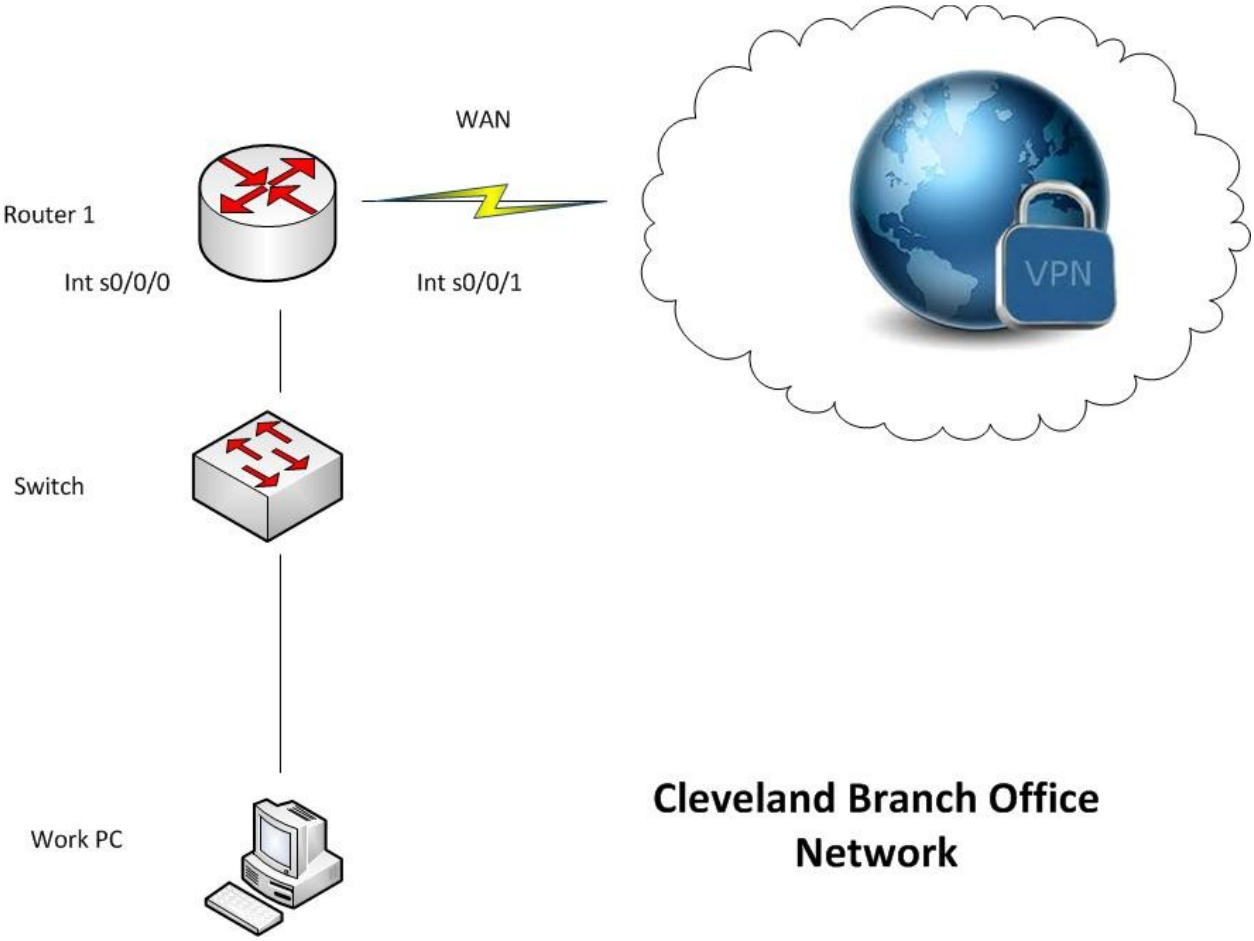
6.0 Revision History

Version 1.0

Example of ACL IOS Configuration:

```
#  Configure terminal
#  Ip access-list extended INVPN
#  Permit tcp 192.168.1.0 0.0.0.255 any eq 1723
#  Permit udp 192.168.1.0 0.0.0.255 any eq 500
#  Permit tcp 192.168.1.0 0.0.0.255 established
#  Permit udp 192.168.1.0 0.0.0.255 established
#  Deny ip any any
#  Ip access-list extended OUTVPN
#  Permit tcp 192.168.1.0 0.0.0.255 any eq 1723
#  Permit udp 192.168.1.0 0.0.0.255 any eq 500
#  Permit tcp 192.168.1.0 0.0.0.255 established
#  Permit udp 192.168.1.0 0.0.0.255 established
#  Deny ip any any
#  Interface s0/0/0
#  Ip access-group INVPN out
#  Interface s0/0/1
#  Ip access-group OUTVPN in
#  exit
```

These commands first open the IOS operating system into global configuration mode and then creates two ACL's. One named INVPN and one named OUTVPN. In this example we are filtering the TTPN VPN packets through TCP port 1723 and UDP port 500. Next, we further filter by an established link, since our VPN (in this example) is on a PVC (permanent virtual circuit). Then, we deny all IP traffic, except the traffic we had originally let pass. In the last four lines, we applied our newly created ACL's to interfaces s0/0/0 inbound and s0/0/1 outbound.



References

Vachon, Bob & Graziani, Rick. (2008). Accessing the WAN.

(pp. 316-317, 322-324, 332-337, 347-357).Indianapolis, IN. Cisco Press.

Computer Networking Notes. (no date). Access Control List Standard Extended. Retrieved from:

http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html

Tech On Tour. (no date). Ports Needed for VPN Passthrough. Retrieved from:

http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html

Sans.org. (no date). Network Security Policy Templates. Retrieved from:

http://www.sans.org/security-resources/policies/network.php