BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang berkembang pesat saat ini, perkembangan teknologi informasi telah menjadi salah satu pilar utama dalam mendukung berbagai aspek kehidupan sehari-hari. Namun, seiring dengan kemajuan tersebut, muncul pula tantangan baru seperti dalam hal keamanan *cyber*. Kejahatan *cyber* semakin canggih dan merugikan, mengancam setiap individu dan perusahaan yang mengandalkan teknologi informasi. Menyadari pentingnya perlindungan terhadap keamanan jaringan di tengah maraknya ancaman *cyber*, PT Datacomm hadir sebagai solusi terpercaya. Perusahaan ini menawarkan layanan keamanan jaringan yang komprehensif untuk membantu individu dan perusahaan melindungi aset digital mereka dari berbagai ancaman *cyber*.

Keamanan jaringan memiliki definisi yaitu tindakan untuk mengamankan serta mengurangi resiko gangguan terhadap *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan)[1]. Dalam laporan ini, berfokus pada aspek *integrity* yaitu dengan menerapan *network access control* (NAC) untuk memastikan bahwa data dan *resource network* pelanggan PT Datacomm hanya digunakan oleh pengguna yang sah dan hanya perangkat yang memenuhi kebijakan keamanan yang diizinkan untuk mengakses jaringan.

Penerapan NAC menjadi penting bagi *customer* PT Datacomm karena dapat memberikan kontrol dan visibilitas yang lebih baik terhadap perangkat yang terhubung ke jaringan. Dengan NAC, dapat memastikan bahwa hanya perangkat yang sesuai dengan standar keamanan yang dapat mengakses jaringan, sehingga dapat mengurangi risiko intrusi dan kebocoran data. Selain itu, NAC juga dapat membantu dalam memantau aktivitas perangkat di dalam jaringan dan melakukan tindakan perbaikan atau mitigasi jika terjadi potensi ancaman.

1.2 Rumusan Masalah

Untuk implementasi *Network Access Control* (NAC), teknologi atau *software* yang akan digunakan adalah Forescout NAC, yang berbasis *Virtual CounterACT Enterprise Manager* (VCEM). Agar dapat mengakses jaringan, pengguna atau perangkat harus mematuhi kebijakan keamanan yang berlaku di Perusahaan *customers* PT Datacomm. Perangkat tersebut harus sesuai dengan standar perusahaan, yaitu sudah ter-*install agent* Secure Connector, antivirus (AV), dan NetBIOS domain yang sesuai dengan kebijakan yang berlaku. Dengan menggunakan Forescout NAC sebagai solusi implementasi *network access control*, diharapkan dapat memastikan hanya perangkat yang memenuhi persyaratan keamanan yang dapat terhubung ke jaringan perusahaan. Hal ini bertujuan untuk meningkatkan keamanan jaringan dan melindungi aset-aset kritis perusahaan *customers* PT Datacomm.

1.3 Tujuan

Tujuan yang akan dicapai diantaranya sebagai berikut:

1. Memastikan hanya perangkat yang memenuhi syarat yang dapat mengakses jaringan internal *customer*.
2. Memberi visibilitas *agar dapat Memonitoring user-user* yang mengakses jaringan internal *customer*.

1.4 Batasan Masalah

Batasan masalah dalam pengembangan sistem ini yaitu:

1. Ruang lingkup Laporan magang ini hanya ada pada *Virtual CounterACT Enterprise Manager (VCEM)* dan *endpoint testing.*
2. Ruang lingkup disisi VCEM hanya di bagian *policy general* dan *policy blocking*.
3. Ruang lingkup disisi *endpoint* hanya melibatkan *endpoint testing* tidak pada *endpoint customer.*

1.5 Penjadwalan Kerja

Untuk memastikan seluruh pekerjaan dapat diselesaikan tepat waktu dan sesuai dengan rencana, penulis telah membuat tabel jadwal pelaksanaan kerja menjadi 2 periode. Berikut adalah tabel jadwal pelaksaan kerja periode 1:

Tabel 1-1 Jadwal pelaksanan kerja periode 1

No	Deskripsi Kerja	Juli 2023				Agustus 2023				September 2023				Oktober 2023				November 2023				Desember 2023			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	*Meeting Project/ Sharing Session*																								
2	*Proof of Concept*																								
5	*Configurasi Perangkat*																								
6	*Monitoring & Report*																								
7	*Preventif Maintenance*																								
8	Pembuatan dokumen kegiataan *config* dll.																								

Berikut adalah tabel jadwal pelaksaan kerja pada periode 2:

Tabel 1-2 Jadwal pelaksanan kerja periode 2

No	Deskripsi Kerja	Januari 2024				Februari 2024				Maret 2024				April 2024				Mei 2024				Juni 2024			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	*Meeting Project/ Sharing Session*																								
2	*Proof of Concept*																								
5	*Configurasi Perangkat*																								
6	*Monitoring & Report*																								
7	*Preventif Maintenance*																								
8	Pembuatan dokumen kegiataan *config* dll.																								